

The Ethics of Government Backdoors in Encryption Systems

Delaney Donaghy

IT489-A Capstone Project

Marymount University

Dr. Osei Hyiamang

September 28, 2025

Abstract

The long standing debate between government duties to protect the public and the civil rights of privacy and liberties has come to a high point with the introduction of government backdoors in encryption systems. In the United States of America, our government exchanges civilian obedience to laws and regulations for the protection of rights, such as individual privacy, freedom of expression, and protection from surveillance. With government encryption backdoors these rights are threatened in the name of ‘protection’ from internal and external threats. This topic highlights the importance of protecting civil rights and liberties and extends the knowledge of how the government is protecting and threatening these rights. The paper aims to cover five objectives. Firstly, it examines the ethical justification for government-mandated encryption backdoors using philosophical theories. Another is assessing how encryption backdoors affect individual rights on a legal framework. Thirdly, it evaluates the technical risks of implementing backdoors, such as weakening security. Additionally, analyzes how governments can ethically balance national security interests with protecting digital rights and public trust. Lastly, reviews real-world examples of government attempts to implement backdoors, including industry and public responses, to assess ethical and societal impacts. The research takes a mixed-method approach with careful analysis. Through the qualitative method, concepts and thoughts regarding government backdoors, encryption, civil rights, and ethical theories are collected. Quantitative data is collected to determine patterns in the research, such as the occurrences of government backdoors and their common target, taken from case studies. By the end of this research, there should be a deeper understanding of the implications and ethics of government surveillance and the technology used to achieve it. A clear resolution to the questions of if governments are ethical in using encryption surveillance techniques to monitor civilians is developed.

Keywords: civil rights and liberties, encryption backdoors, ethics, national security, surveillance.

Table of Contents

| | |
|---|-----------|
| Abstract | 2 |
| Table of Contents | 3 |
| List of Figures | 5 |
| List of Tables | 5 |
| Chapter 1: Introduction | 6 |
| Overview | 6 |
| Problem Statement | 8 |
| Research Objectives | 8 |
| Research Questions | 9 |
| Significance | 10 |
| Existing Gaps and Need for the Research Topic | 11 |
| Keywords Definitions | 12 |
| Organization of the Remaining Chapters | 13 |
| Chapter 2: Literature Review | 14 |
| Overview | 14 |
| Literature Search Strategy | 16 |
| Literature Findings | 17 |
| Government Backdoors and their Risks to System Integrity and User Trust | 17 |

| | |
|--|-----------|
| GOVERNMENT BACKDOORS IN ENCRYPTION SYSTEMS | 4 |
| Ethical Principles Applied | 19 |
| Existing Legal Frameworks on Government Surveillance and Digital Privacy | 22 |
| Citizen Protection versus Digital Privacy | 24 |
| Summary | 27 |
| Chapter 3: Research Methodology | 28 |
| Overview | 28 |
| The Rationale for the Research Approach | 30 |
| Contextualize the Study | 31 |
| Research Objectives | 31 |
| Research Questions | 32 |
| Data Collection Methodology | 32 |
| Data Analysis Plan | 33 |
| Trustworthiness | 35 |
| Ethical Considerations | 36 |
| Summary | 37 |
| Chapter 4: Data Analysis | 39 |
| Overview | 39 |
| Data Results | 40 |
| Government Backdoors and their Risks to System Integrity and User Trust | 42 |
| Technical and Security Risks of Backdoors | 43 |
| Ethical Principles Applied | 43 |

| | |
|--|-----------|
| GOVERNMENT BACKDOORS IN ENCRYPTION SYSTEMS | 5 |
| Ethical Evaluation Frameworks | 44 |
| Existing Legal Frameworks on Government Surveillance and Digital Privacy | 45 |
| Legal and Regulatory Patterns | 45 |
| Citizen Protection versus Digital Privacy | 46 |
| Public Sentiment and Societal Perceptions | 47 |
| Ethical Justifiability of Government Backdoors | 48 |
| Summary | 48 |
| Chapter 5: Discussion, Recommendations, & Conclusions | 51 |
| Summary of the Results | 51 |
| Interpretation of Findings | 52 |
| Limitations of Study | 55 |
| Recommendations | 56 |
| Conclusion | 57 |
| References | 59 |

List of Figures

| | |
|----------------------------------|----|
| Public Concern Over Data Privacy | 47 |
|----------------------------------|----|

List of Tables

| | |
|--|----|
| Post-Data Cleansing Source Categories | 41 |
| Summary of Technical Findings | 43 |
| Comparison of Ethical Framework Outcomes | 44 |
| Comparative Overview of Legal Trends | 46 |

Chapter 1: Introduction

Overview

The digital era has fundamentally transformed the way individuals communicate, store information, and engage with the world. As a result, cybersecurity and data privacy have become central to both public discourse and government policy. Encryption, a form of digital security technology, enables individuals and organizations to protect sensitive information from unauthorized access (Paula Bernardi & Celia Richardson, 2025). However, the rise of encrypted communication can also present challenges for law enforcement and national security agencies. It is possible that criminals can exploit encryption to hide illegal activities. In response, “more and more governments are jumping on the bandwagon of demanding encryption backdoors” (Bernardi & Richardson, 2025). These backdoors will allow authorized individuals to closely monitor and collect selective data.

While these government-mandated backdoors are typically justified on the grounds of national security, their ethical implications have raised significant concerns. On one hand, some may argue that backdoors are necessary to investigate and prevent criminal and terrorist activities, ultimately protecting society at large. On the other hand, critics emphasize “once a vulnerability exists, communication is no longer secure. This is why creating backdoors weakens encryption for everyone... with no guarantee that it would actually affect the criminals they claim to be targeting”(Bernardi & Richardson, 2025). Furthermore, backdoors threaten the civil liberties of individuals, particularly the right to privacy, freedom of expression, and protection from unwarranted surveillance. These conflicting perspectives raise a fundamental ethical question, Can government-mandated encryption backdoors be morally justified in a society that values both security and individual rights?

This research paper aims to critically examine that question by engaging with ethical philosophy, technical analysis, legal frameworks, and real-world case studies. The study incorporates classical ethical theories such as utilitarianism, deontology, and other rights-based ethics, to evaluate the moral justification for government access to encrypted systems. By focusing the discussion in well-established moral theories, the research moves beyond surface-level arguments and provides a more in-depth understanding for assessing the ethical implications of backdoors.

The paper delves into a number of key case studies in which governments have attempted to mandate encryption backdoors. These cases illustrate how technology companies, cybersecurity experts, civil rights advocates, and the general public have responded to government surveillance demands. By examining these responses, the study aims to uncover patterns of resistance, compliance, and compromise, and to assess how public view and corporate responsibility shape the ethics of surveillance.

In addition to philosophical and case-based analysis, the paper examines international legal frameworks that address the balance between digital privacy and state surveillance. This includes an overview of how various countries regulate encryption, data access, and digital rights. These comparisons highlight diverse approaches to surveillance and the role of legal safeguards in protecting civil liberties.

Ultimately, the goal of this research is not only to determine whether encryption backdoors are ethically justifiable, but also to contribute to the broader conversation about digital rights in the modern technological world. As technology continues to advance, the decisions made today about surveillance, security, and privacy will shape the future of governance, civil liberties, and public trust. By providing a well-reasoned ethical framework grounded in both

theory and real-world evidence, this study aims to guide policymakers, developers, and the public in navigating the balance of security and freedom in the digital age. While the research acknowledges the real and pressing threats of national security, it seeks to find a balanced solution that respects ethical boundaries and practical concerns. This paper aims to increase public discourse on government mandated surveillance and digital data protection to aid in the conversation of setting a precedent on technological freedoms.

Problem Statement

As governments worldwide seek greater access to encrypted communications for national security and law enforcement purposes, the push for mandated backdoors in encryption systems has sparked intense ethical, legal, and technical debates. While some may argue that such access is essential for catching crime and terrorism, others warn that backdoors inherently compromise user privacy, civil liberties, and the overall security of digital systems. The ethical implications of these measures remain challenged, particularly when weighed against individual rights and the potential for abuse or exploitation. This research aims to explore whether government-mandated encryption backdoors can be ethically justified, considering philosophical ethical theories, real-world case studies, and the potential societal consequences of weakening digital security.

Research Objectives

The paper focuses on five objectives. The first is to examine the ethical implications of government-mandated backdoors in encryption systems. This involves analyzing the philosophical theories such as utilitarianism, consequentialism, deontology, and rights-based ethics, to evaluate the justification of such backdoors.

Another objective assesses the impact of encryption backdoors on individual privacy and civil liberties. It explores how a user's natural rights, privacy, freedom of expression, and protection from surveillance, may be affected by backdoors.

The study additionally evaluates the security risks and technical consequences associated with implementing backdoors. This includes how government involvement with backdoors can cause systems to be exploited by malicious actors and overall weaken cybersecurity for users.

The fourth objective analyzes the balance between national security interests and ethical responsibilities in policymaking. It aims to help determine how governments can ethically pursue security objectives without violating public trust or digital rights.

Lastly, the paper inspects real life case studies of instances where governments have made attempts at securing backdoor access. These case studies reveal how technology organizations and cybersecurity experts reacted and retaliated against the backdoors and the public's thoughts.

Furthermore, the study uses real case studies and philosophical theories to judge the ethics of government backdoors in encryption systems and the impact they have on civilian rights and liberties.

Research Questions

Five questions guide the paper's research and analysis. The first question is, What are government backdoors and what are the risks of system integrity and user trust? Through this question it is discussed what encryption backdoors are and why the government is implementing them. It then goes on to explain the technical consequences of such actions.

The second question is, How can ethical principles of utilitarianism, deontology, and other right-based ethical theories be applied to the debate over encryption backdoors? This

section focuses on ethical theories and philosophers. It analyzes popular theories related to rights and privacy, and applies them to the use of encryption backdoors for government surveillance. Each theory has been examined and their philosophy determines if those who follow, would find backdoors as ethically sound or not.

The third question is, How do international legal frameworks address the tension between government surveillance and digital privacy? Through this question, the paper analyzes existing laws and policies in various governments to determine if any address digital privacy and government surveillance. It notes what guidelines, restrictions, regulations, or boundaries governments may have set to protect their citizens privacy and prevent abuse or on the other hand, to aid in their pursuit to mandate backdoors.

The fourth question is, Should the protection of citizens from harm (e.g., terrorism) outweigh the right to digital privacy? With the excuse of government surveillance being to catch and prevent crime and terrorism, it begs the question of if citizens should give up their right to privacy in return. This question tackles if the good of a whole population in face of a hypothetical outweighs the good of the individual.

The main question and challenge is, Is it ethically justifiable for governments to mandate backdoors in encryption systems for national security purposes? This question covers the whole premise of the research. Each of the other questions offer insight and the knowledge gained is carefully compared and contrasted to develop a resolution on the overall problem.

Significance

The research should result in an increased understanding of government encryption backdoors. Furthermore, it draws the collective thoughts of the topic within those involved. Including companies, the public, and the government. The philosophy research brings insight on

the most common philosophical theories on civil rights and liberties. These theories can be compared to backdoors and establish if they compromise the rights of citizens or if governments are justified in their actions. This paired with the thoughts of those involved allows a careful analysis of the philosophical preference of each individual group. This research can explain why each group agrees or disagrees with the implementation of government backdoors. The research as a whole dissects the ethics of government backdoors and it determines whether or not they can be justified. Furthermore, it should be able to determine if this subject is a growing threat or if it may be instead something civilians and organizations have to accept and adapt to. It also determines how, when, and if future actions need to be taken to crack down on government backdoors.

Existing Gaps and Need for the Research Topic

While most debates regarding encryption backdoors focus on legal or technical concerns, there is little consideration for ethics. The ethical implications are greatly underexplored or treated superficially. A more interdisciplinary approach integrates perspectives of ethics, law, and cybersecurity holistically. With the constant tension between national security and individual rights, there is a lack of definite boundaries. Especially with the rapidly growing digital landscape, there is little consensus on where to draw the line.

Furthermore, real-world case studies often lack well developed analysis. For the few known instances where governments have requested or implemented backdoors, there is low comprehensive and critical analysis of the cases including the public and industry reactions.

With the fast evolving technical climate, there is a need for grounded ethical insights to aid policymakers in making ethically guided legislation. An ethical framework in legal fields will protect citizens, developers, and tech companies from governments increasing demands.

There is also a lack of public debate and opinion on digital data surveillance. As public trust declines in digital systems due to surveillance threats, this research may bring clarification on the ethics to light. It aids in the discussion, involvement, and civic participation in digital rights discourse. It is important for citizens to understand their rights and be educated on the effects of government surveillance on their intellectual property and personal data. Having these conversations allows the public to make informed decisions and discuss if action needs to be taken to deter government advances in surveillance.

Applying these ethical theories to real-world occurrences provide actionable insights and balance moral principles with government legislation in the modern digital age.

Keywords Definitions

Civil rights and liberties: Civil rights are rights “secured by positive government action, often in the form of legislation...given and guaranteed by the power of the state.” Civil liberties are “freedoms that are secured by placing restraints on government”(Rebecca Hamlin, 2025). In regards to this paper, the civil rights and liberties that are focused on are privacy, digital property, and protection from surveillance.

Encryption backdoors: Encryption backdoors are “a type of exceptional access that a platform gives third parties– such as law enforcement and government officials– to the content of encrypted communications” (Paula Bernardi & Celia Richardson, 2025). The encryption backdoors that are referred to in the research are government mandated and used for surveillance.

Ethics: Ethics are “the discipline concerned with what is morally good and bad and morally right and wrong. The term is also applied to any system or theory of moral values or

principles” (Peter Singer, 2025). The ethics concerned in this paper are applied to privacy in consideration to government surveillance.

National security: National security is the “protection of a nation’s sovereignty, its territorial integrity, its citizens, and its established way of life from various threats” (LegalClarity, 2025). This paper refers to national security as what is being protected through encryption backdoors as surveillance techniques.

Surveillance: The Cambridge dictionary defines surveillance as “the careful watching of a person or place, especially by the police or army, because of a crime that has happened or is expected” (2025) The research uses surveillance to describe the government's use of encryption backdoors to monitor digital data for criminal and terrorist activity.

Organization of the Remaining Chapters

The remaining chapter of the research consists of four sections.

Chapter 2: Literature Review. Here the sources previously collected and analyzed are described and summarized within applicability to the project. The sources are thoroughly discussed and frame what is known and unknown about the topic of study. The project fills the gap that is found within the literature review and extends knowledge within the field.

Chapter 3: Research Methodology. This section describes the organization and details the steps used to achieve and analyze the data. It documents the methods and processes used to collect and analyze the sources.

Chapter 4: Data Analysis. During the data analysis, the data collected through the literature review are analyzed and documented in relation to the field of study.

Chapter 5: Discussion, Conclusion, and Recommendations. In this section, a conclusion is found and discussed based on the findings.

Chapter 2: Literature Review

Overview

This chapter provides a critical examination of the ethical, legal, and societal debates surrounding government backdoors in encryption systems. It reviews current scholarly articles to establish a foundation for understanding how privacy, security, and governance intersect in the digital age. The central aim is to determine whether state efforts to access encrypted communications for national security and law enforcement can be ethically justified without undermining public trust or the integrity of digital systems. Drawing from philosophy, law, and cybersecurity, the chapter draws on different perspectives that reveal the complexity of balancing collective safety with individual rights.

The chapter begins by outlining the literature search strategy, detailing the use of databases such as Google Scholar and the Marymount Library catalog to locate relevant academic, governmental, and institutional publications. The search was limited primarily to works published between 2021 and 2025, with a few earlier texts included for their enduring ethical or theoretical value. Key search terms, including *government backdoors*, *digital privacy*, *ethical theory*, and *surveillance law*, ensured a comprehensive and focused review. This methodology provided the basis for selecting sources that collectively explore the technological, philosophical, and legal framework of encryption policy.

The first topic section, *Government Backdoors and their Risks to System Integrity and User Trust*, addresses the technical complications and cybersecurity implications of government access. Scholars like Bernardi and Richardson (2025) explain how backdoors, even when intended for authorized use, create vulnerabilities exploitable by malicious actors. Forno (2025) illustrates these risks through real-world cases such as the FBI's and U.K. government's attempts

to compel Apple to weaken its encryption systems, highlighting how corporate resistance has become a focal point in the privacy–security debate. These studies emphasize that government backdoors, while framed as tools for protection, can paradoxically weaken overall digital safety and erode public trust.

The second section, *Ethical Principles Applied*, evaluates the backdoor debate through utilitarian, deontological, and rights-based frameworks. The Lawcenta Team (2024) applies a utilitarian lens, arguing that privacy restrictions are only justifiable when the societal benefits clearly outweigh the harms. Prabhumoye et al. (2021) offer a deontological critique, contending that embedding backdoors violates moral duties of autonomy and consent by treating users as means to state ends. Talbott (2013) bridges these perspectives by asserting that long-term respect for human rights produces the best societal outcomes, suggesting that institutionalizing surveillance may ultimately harm both trust and collective welfare. Together, these ethical approaches bring to light the complexity of balancing individual rights with state interests in security.

The third section, *Existing Legal Frameworks on Government Surveillance and Digital Privacy*, situates the ethical debate within the context of evolving laws in the United States and United Kingdom. GovFacts (2025) traces the extension of constitutional privacy rights into digital contexts through landmark cases like *Katz* and *Carpenter*, while also examining post-9/11 legislation that expanded surveillance powers. Broadbent (2024) analyzes recent U.K. amendments granting the government authority to review or delay encryption upgrades, underscoring growing concerns about state overreach. These legal analyses reveal persistent gaps between technological advancement and adequate oversight, as governments struggle to modernize privacy law without undermining fundamental rights.

The final section, *Citizen Protection versus Digital Privacy*, explores public perception and the ethical legitimacy of surveillance in democratic societies. McClain et al. (2023) demonstrate widespread public concern over both corporate and government data collection, coupled with a sense of powerlessness and low trust. Classic arguments from Kobrin and Donaldson (1999) and more recent analyses by Scott and Ó Floinn (2024) further stress that while privacy is not absolute, any intrusion must remain proportionate, transparent, and subject to strict accountability. These findings underscore that public consent and confidence are essential to ethical governance in the digital sphere.

Taken together, the reviewed literature exposes a recurring tension between national security imperatives and the preservation of individual autonomy. While proponents of government access argue for its necessity in preventing harm, most scholars warn that backdoors create systemic vulnerabilities and threaten democratic trust. The chapter concludes that the question of government backdoors is not merely technical or legal—it is fundamentally ethical. By integrating philosophical reasoning with empirical and legal evidence, this review establishes the groundwork for the succeeding analysis, which evaluates whether the pursuit of citizen protection can ethically outweigh the obligation to maintain secure and private digital communication systems.

Literature Search Strategy

The literature sources applicable to this topic are found through various methods and tools. Research databases such as Google Scholar and the Marymount catalog database are utilized in addition to government sites and other universities publications. Some papers may be found through the citations of other, initial sources that provide relevance to the topic at hand.

Google scholar is used as a free academic search engine to find scholarly literature across political and technological disciplines. Google scholar includes articles, research, theses, and books. It aids in avoiding irrelevant and unreliable sources and results in the literature search.

The Marymount catalog and MULibrary Search offers an easy way to search for books, government documents, journals, articles, and other media over the internet and what is available in-person at the Reinsch Library or nearby locations. The Marymount Catalog also offers Librarian assistance through an online chat feature to aid in the research process.

The subject matter that was used in the search directly relates to the topic and was restricted to publications within the past five years, from 2021-2025. That is with the exception of two publications: *Consequentialism and Human Rights* by William J. Tailbott (2013) and *The Debate on Privacy Protection: Should it be Unlimited?* by Stephen J. Kobrin and Thomas Donaldson (1999). Key themes used in the search include, government backdoors, ethical theories, existing legal frameworks, and public debates.

Literature Findings

The following literature findings are used to establish basic knowledge and understanding of major themes in this research project. The sources and material found are used to answer research questions and later developed to be analyzed in regards to the topic at hand.

Government Backdoors and their Risks to System Integrity and User Trust

Paula Bernardi and Celia Richardson (2025) provides a basic overview of what encryption backdoors are and the technical and societal risks posed by government-mandated backdoors in encryption systems. The authors define a backdoor as “type of exceptional access that a platform gives third parties– such as law enforcement and government officials– to the content of encrypted communications.” They describe backdoors as a sort of ‘middle box’ that

intercepts data, decrypts it, then re-encrypts the packets to send it to the intended recipient. It is compared in sharp contrast to end-to-end encryption where only the sender and receiver have access to the unique decryption key. The authors warn that although backdoors may be accessed only by authorized users, it still creates a vulnerability that can be exploited by malicious actors. Bernardi and Richardson argue that backdoors inflict the opposite of their intended purpose and put millions of citizens at risk.

Richard Forno (2025) offers examples of real-world government backdoor attempts and the societal impact of them. The author introduces the concept of the ‘Clipper Chip’ which allows government access to encryption systems through a third party for law enforcement or national security needs only. Companies such as Google and Apple have been proposed by governments to build similar systems as the “Clipper Chip.’ Forno details in 2016, the FBI requested Apple to create a tool to break the encryption of an iPhone owned by a suspected terrorist. Apple was involved in another case with the U.K. government in 2025, who ordered a backdoor to be placed worldwide. In both cases, Apple refused to comply with government demands and chose instead to defend their users' privacy and security.

Richard Forno (2025) explains in his paper the reasons behind the push for government mandates. In addition to terrorist actions, he notes “scanning for child sexual abuse material is a controversial concern when encryption is involved (2025).” Forno describes the conflicting public views Apple has received over device scanning. While some argue that it violated privacy stances, others stress the need for better protection of children. The author rationalized the ‘valid concern’ regarding child safety however doubles down on the perspective of cybersecurity and the vulnerabilities created by backdoors.

Ethical Principles Applied

The Lawcenta Team (2024), lay out a utilitarian framework for evaluating and shaping privacy laws so as to maximize social welfare while weighing individual rights. They begin by defining the ethical foundations of privacy law: autonomy, dignity, and the prevention of harm to individuals, and then argue that utilitarian ethics, focused on maximizing overall good, can help policymakers when balancing privacy protections against societal benefits such as security, innovation, public health, and efficiency. The article recommends several key principles: proportionality in privacy restrictions (i.e. privacy intrusions should only occur when the benefit is large enough), transparency, accountability, continuous evaluation, and inclusive public engagement, especially including marginalized groups.

The authors also discuss how utilitarian evaluation might work in practice: measuring benefits (e.g. crime reduction, public health improvements) and quantifying likely harms (e.g. discrimination, loss of autonomy or trust) in order to make more empirically grounded policy choices. They offer real-world cases (for example, the U.S. Supreme Court's *Kyllo v. United States*, and the invalidation of the Privacy Shield by the European Court of Justice) to show how courts have implicitly or explicitly used utilitarian reasoning in privacy or surveillance-law disputes.

However, the article also acknowledges substantive limitations: utilitarianism may overlook the harms experienced by marginalized or vulnerable populations; quantification of benefits and harms is difficult, especially when harms are long term or intangible, and utility-based frameworks can risk justifying privacy intrusions if the perceived benefit to the majority is large enough, even if the costs to individuals are significant.

Overall, the Lawcenta Team frames utilitarian ethics as a possible guide to arguments supporting government backdoors: while backdoors might be defended on the grounds of societal benefits (e.g., law enforcement, national security), a utilitarian framework requires assessment of all harms. This includes trust, system integrity, privacy, risk to minorities and not just majority benefit. Therefore it adds nuance to analyzing the ethical risks of backdoors by insisting that benefits must significantly outweigh likely harms and that certain harms may be grave even if less quantifiable.

Prabhumoye et al., (2021) engages deontological moral theory to examine algorithmic systems by focusing on two central principles: the generalization principle and respect for autonomy via informed consent. The authors argue that an action is morally permissible only if one can rationally will that the maxim underlying it be a universal rule or generalization, and that ethical design must treat individuals not merely as means but as ends. Through case studies in NLP, they reveal how certain system behaviors, such as silently handling ambiguous content or making invasive inferences, would fail the generalization test due to violating trust and reliability and infringing on users' autonomy.

Switching the perspective to encryption and government backdoors, the deontological lens from Prabhumoye et al. offers potent critiques. First, the generalization principle disfavors the adoption of backdoors because if every encryption system contained such access points, the universal rule would be “no communication is ever truly private or secure,” defeating the very purpose of encryption and undermining baseline trust. The maxim “design systems with government exceptional access” cannot be willed universally without violating confidentiality. Second, respect for autonomy demands that users be meaningfully informed of how and when backdoors may be used, along with the attendant risks. In practice, backdoor proposals often fail

to offer that level of transparency or consent, treating users as means to state surveillance. The act of embedding a backdoor, even for legitimate ends, violates the duty not to treat users merely as instruments. This paper shifts the debate from weighing overall outcomes (e.g. security vs privacy) to asking whether certain system designs are inherently incompatible with moral duty, agency, and respect for individuals.

William J. Talbott (2013), examines the tension between consequentialist moral reasoning and rights-based ethics, arguing that human rights can be understood through a “second-order” consequentialism. Rather than focusing on individual actions, Talbott suggests evaluating moral systems based on the broader social outcomes produced by institutions and laws. He uses this framework to compare utilitarian goals of maximizing well-being with the non-negotiable nature of human rights, declaring that a rights-respecting system can produce the best long-term consequences for society. This view challenges both strict utilitarianism, which allows rights violations for aggregate benefit, and rigid deontological approaches that ignore outcomes altogether.

Applied to the debate on government backdoors in encryption, Talbott’s consequentialist framework offers a lens through which to balance privacy and security without harming foundational human rights. Mandating backdoors might appear justified if it prevents harm or enhances collective safety, yet Talbott’s argument warns that the systemic consequences, loss of trust, vulnerability to abuse, and long-term degradation of individual autonomy, may outweigh these short-term gains. His approach underscores that ethical policymaking must assess not just immediate security outcomes but also whether the institutionalization of surveillance practices aligns with the broader well-being and dignity that human rights aim to protect.

Existing Legal Frameworks on Government Surveillance and Digital Privacy

Govfacts, (2025) outlines the tensions and legal frameworks that mediate government surveillance and constitutional privacy rights in the United States. The article centers around the Constitution's Fourth Amendment, which "protects against unreasonable searches and seizures." The authors emphasize the need to now interpret the amendment in light of digital technologies such as telephones and the internet. It then traces key legal developments, such as *Katz v. United States*, which extended Fourth Amendment protection to expectations of privacy rather than just "places," and *Carpenter v. United States*, which constrained warrantless access to cell-site location information (CSLI). These developments show how courts have extended constitutional norms into the digital age. The article also catalogs statutory frameworks that expanded surveillance authority post-9/11: the USA PATRIOT Act with Section 215, FISA and its Section 702 program, which includes "backdoor searches", national security letters, and "sneak-and-peek" warrants. All of which push into legal gray zones or expand exceptions to traditional warrant requirements.

The GovFacts article highlights the gaps, tensions, and oversight challenges embedded in the current legal architecture. It underscores how the law often lags behind emerging technologies, creating periods of legal uncertainty or overreach. For example, when new surveillance tools are used before the courts rule on their constitutionality. It also discusses oversight mechanisms, like the Foreign Intelligence Surveillance Court (FISC), congressional intelligence committees, inspectors general, and the Privacy and Civil Liberties Oversight Board (PCLOB), while noting critiques that many of these bodies operate under secrecy, limited adversarial review, or institutional weakness. Alongside the legal narrative, the article describes real harms, such as documented abuses of surveillance power, infringement on civil liberties,

effects on free speech, and questions about whether government claims of effectiveness justify the tradeoffs to privacy.

Broadbent(2024), analyzes significant amendments made in the UK's Investigatory Powers (Amendment) Act 2024, which replaces the existing Investigatory Powers Act of 2016 (IPA 2016). The author details how the UK government justifies these amendments as necessary responses to technological changes, increasing volumes of data, and new kinds of communications and devices. These amendments are to fill perceived gaps in law enforcement's ability to access communications or metadata under existing legal regimes. Broadbent outlines several key modifications, most notable are notification requirements that obligate companies to tell the Secretary of State before introducing stronger encryption or other security improvements. In some cases, it allows suspension of such changes pending government review. This gives the UK government effective veto powers over technological changes that could disable "exceptional access" to data.

However, the article emphasizes risks and critiques of the new legal framework. Especially its potential to weaken user security, decrease trust, and distort market incentives. Broadbent notes concerns that forcing private firms to report planned encryption upgrades, and possibly delay them, may slow development of better security, reduce confidence in UK-based services, and impose legal conflicts for international firms caught between UK mandates and privacy or data protection laws elsewhere. The author concludes that while the amendments may expand the government's abilities to surveil, they risk undermining fundamental rights, weakening trust in digital systems, and harming the UK's attractiveness as a center for secure tech innovation.

Citizen Protection versus Digital Privacy

Mcclain et al., (2023) present evidence obtained from surveys on how U.S. citizens perceive the risks to their personal data, their sense of control, or lack thereof, and their sentiment toward regulation. The survey of 5,101 U.S. adults reveals an asymmetry array of data. While 81% of respondents express at least some concern about how companies use their data, 71% are concerned about government use. More tellingly, large majorities feel nearly powerless with 73% saying they have little or no control over how companies handle their data, and 79% feel similarly about governmental data collection. The survey also indicates a steep increase in public unease since 2019. The share of Americans reporting low understanding of how companies use their data has grown from 59% to 67%, while concern over government data use rose from 64% to 71%. (Mcclain et al., 2013).

More than just documenting attitudes, the report underscores the normative demand for policy. 72% of respondents say there should be more regulation of what companies can do with personal information. Despite this, the report also exposes a gap between perception and efficacy with 72% admitting they have little or no understanding of existing privacy laws and regulations, representing an increase from 63% in 2019. Moreover, most Americans view privacy policies as inadequate. 61% say they are “not too” or “not at all” effective at communicating how data is used. These findings suggest that citizens demand protective oversight yet feel both uninformed and structurally disempowered. In the tension between citizen protection and digital privacy, this uncertainty complicates the legitimacy of surveillance measures. Even if some government actions are defended as protective, public skepticism and perceived transparency may decrease trust and moral authority. (Mcclain et al., 2013).

Stephen J. Kobrin and Thomas Donaldson (1999), present a public lecture by Amitai Etzioni, a leading figure in communitarian political thought, exploring the idea that society must sometimes limit individual privacy for the sake of public welfare. The article frames the core argument, while most people instinctively value privacy, there exist circumstances, such as protecting children from abuse or preventing serious crime, in which intrusions may be justified. Etzioni claims that privacy is not an absolute right, but rather one whose boundaries must be drawn in light of collective needs. He argues that public policy should aim for “minimal intrusion” solutions where possible, giving the examples of traffic cameras capturing license plates rather than full imagery, so as to balance societal security goals with individual privacy protection. Kobrin and Donaldson also warn of the danger of using the public-good rationale as a blank check. With expansions of surveillance in the name of safety risk overcoming societal boundaries if not constrained by clear ethical and legal frameworks.

Kobrin and Donaldson provide a baseline that aligns with the “citizen protection vs. privacy” question. Etzioni’s arguments offer a defense of some surveillance authority, but within a restricted, rights-sensitive framework. This suggests that proponents of encryption backdoors might be justified but must guard against the sliding scale that allows justifications to harm core privacy protections. More critically, the article underscores that policy design matters. It is not enough to claim security benefits, any intrusion must be proportionate, transparent, and subject to safeguards. In the debate over backdoors, this means that even if a government argues that backdoors are necessary to prevent harm, such a claim cannot automatically override the right to digital privacy. Instead, it must be defensible in terms of minimal interference, oversight, and accountability. This article introduces a moderating position between absolutist privacy and

maximal surveillance and demands principled limits rather than clear domination of security over privacy.

Paul F. Scott and Michael O Floinn (2024), investigates the evolving legal and policy regime surrounding backdoors to encryption in the UK, distinguishing between “technical backdoors,” deliberate design or vulnerability that enables bypassing encryption, and “legal backdoors,” laws or mandates requiring companies to make data accessible. The authors trace how the UK government has attempted to balance national security needs, such as combating serious crime and terrorism, with digital privacy rights, especially under the European Convention on Human Rights (ECHR), the UK’s Human Rights Act, and emerging obligations under data protection laws. They examine key legislative efforts and the legal reasoning used in courts to justify or reject compulsory access in various forms.

A central claim from the article is that while legal frameworks increasingly recognize the importance of privacy, they also provide for significant exceptions under tightly defined conditions. The authors analyze whether these exceptions are sufficiently constrained to prevent overreach. They find that legal backdoors often come with oversight mechanisms, judicial or independent, requirement for proportionality, and necessity in a democratic society. However, they also identify risks, including vague definitions of “serious crime,” weakening of encryption standards, and effects on free speech. Importantly, the authors argue that while citizen protection is a legitimate aim, it should not automatically outweigh the right to digital privacy. Rather, any infringement must satisfy legal tests of necessity, proportionality, transparency, and accountability. In their analysis, Scott and Ó Floinn lean toward the view that preserving strong encryption and privacy is essential, and that policy designs which elevate security to a point where privacy is threatened are ethically and legally problematic.

Summary

The information gathered from the reviewed sources are used to examine how the debate over government backdoors in encryption systems reflects broader questions of digital privacy, security, and ethical governance. The literature provides insight into both the practical risks and philosophical arguments surrounding government access to encrypted data. Many of the works analyze the balance between protecting citizens from harm and upholding the right to privacy in the digital era. These perspectives support the argument that government backdoors, while often justified as tools for law enforcement and counterterrorism, ultimately introduce vulnerabilities that threaten both personal security and societal trust. Some sources, however, suggest that limited, highly regulated access may be ethically defensible if it demonstrably prevents significant harm, a claim that is evaluated in the analysis portion of this paper.

Additional research also explores how existing legal and ethical frameworks attempt to navigate the tension between surveillance and privacy. Studies addressing utilitarian, deontological, and rights-based ethics offer contrasting interpretations of when, if ever, privacy should yield to state interests. Legal analyses from the U.S. and U.K. further demonstrate how governments have expanded surveillance powers while attempting to preserve public accountability. These sources collectively reveal a growing global concern about maintaining both safety and digital integrity in an interconnected world. Understanding these perspectives is essential to determining whether the protection of citizens can ethically justify the corruption of encryption safeguards and the potential loss of individual digital privacy.

Chapter 3: Research Methodology

Overview

The purpose of this research is to critically examine the ethical implications of government-mandated encryption backdoors within digital communication systems. As governments worldwide increasingly seek access to encrypted data for national security purposes, the tension between state surveillance capabilities and individual privacy rights has intensified, creating significant ethical, legal, and technical challenges.

This study seeks to provide a comprehensive analysis of these challenges by exploring the philosophical foundations that guide debates within the various topics of government surveillance. These topics include, encryption backdoors, evaluating the legal frameworks that govern surveillance practices, assessing the technical vulnerabilities introduced by backdoor implementations, and examining real-world cases where governments have attempted to mandate such access.

The significance of this research lies in its contribution to the ongoing discourse surrounding digital rights, cybersecurity, and the ethical responsibilities of governments in an increasingly interconnected world. By systematically analyzing multiple perspectives, from utilitarian and deontological ethical theories to legal precedents and technical security assessments, this study aims to provide a balanced understanding of whether and how governments can ethically justify requiring access to encrypted communications.

This methodology chapter outlines the research approach, data collection strategies, and analytical procedures employed to address the complex ethical questions of this study. The chapter is structured to provide transparency and clarity regarding how the research was conducted, ensuring that findings are credible, valid, and reliable. It begins by establishing the

rationale for using qualitative research methods, explaining why this approach is particularly suited to exploring ethical debates that hinge on diverse values, principles, and contextual factors rather than quantifiable metrics. Following the rationale, the chapter contextualizes the study by presenting the specific research objectives and questions that guide the inquiry, establishing a clear framework for understanding what the research seeks to accomplish.

The research design chosen for this study is qualitative, focusing on an extensive literature review and thematic analysis of existing scholarly work, government publications, legal documents, and policy discussions. This approach was selected because the research questions center on ethical reasoning, moral principles, and normative arguments, all areas where qualitative methods excel.

Unlike quantitative research, which would seek to measure public opinion numerically or statistically analyze surveillance outcomes, this qualitative approach allows for deep engagement with philosophical theories. Using theories such as utilitarianism, deontology, and rights-based ethics, to explore how these frameworks apply to the specific issue of encryption backdoors.

The study's reliance on secondary data is justified by the need to synthesize existing knowledge across multiple disciplines and to build upon established theoretical foundations. This qualitative design is particularly appropriate given the study's objectives: examining ethical justifications using established philosophical theories, assessing legal frameworks, evaluating technical risks, analyzing the balance between national security and digital rights, and reviewing real-world examples. These objectives require interpretive analysis and critical evaluation of existing arguments rather than experimental manipulation or statistical correlation.

The sections that follow show a detailed explanation of the data collection methodology, including the specific databases and search strategies used to identify relevant scholarly

materials, the criteria for source selection, and the rationale of included publications. The chapter then describes the data analysis plan, outlining how thematic analysis is conducted to identify patterns, categorize arguments according to ethical frameworks and disciplinary perspectives, and systematically compare viewpoints to reveal areas of consensus and disagreement.

Subsequent sections address trustworthiness, explaining how credibility, validity, and reliability are maintained throughout the research process, and discuss ethical considerations, detailing how the research adheres to academic integrity standards and responsible scholarship practices.

By providing this comprehensive methodological framework, the chapter ensures that the research process is transparent and aligned with established standards for academic research. The methodology serves not only as a procedural guide but also as a means of establishing the study's legitimacy and scholarly rigor, demonstrating that the findings are the result of systematic inquiry founded in credible sources and guided by consistent analytical principles. Ultimately, this methodological approach enables the research to contribute meaningfully to the critical conversation about the ethics of government mandated surveillance in the digital age.

The Rationale for the Research Approach

When researching a topic such as the ethics regarding government backdoors it is important to use the appropriate research methods to develop an extensive and broad foundation of data to build upon. The rationale behind the methodology ensures credibility of the sources, addresses the gap in the research, and explains the significance of the research.

Qualitative Research Methods: Qualitative research revolves around gathering different experiences, perspectives. Thoughts, and feelings on a specific topic. While quantitative research aims to collect numerical and statistical data, qualitative research focuses on the societal and culture contexts. The renowned social scientist, Robert K. Yin states the most defining features

of qualitative research are, “1. Studying the meaning of people’s lives, in their real-world roles; 2. Representing the views and perspectives of the people (labeled throughout this book, as the participants) in a study; 3. Explicitly attending to and accounting for real-world contextual conditions; 4. Contributing insights from existing or new concepts that may help to explain social behavior and thinking; and 5. Acknowledging the potential relevance of multiple sources of evidence rather than relying on a single source alone” (Yin, 2015, p.9).

When collecting data to support claims within an ethics research project, such as this one, it is important to gather many perspectives and beliefs. Through qualitative research, the researcher can collect varying theological perspectives in regards to privacy and surveillance. Furthermore, the research explores different experiences and thoughts of government backdoors within encryption systems. These experiences stem from various countries, incidents, and demographics.

Contextualize the Study

Contextualizing the study creates a framework for data collection. It brings together the conditions of the research to the research objectives and questions. It approaches the project in a way to link the goals of the study to the reasons behind the methodology choice.

Research Objectives

The design of the research is guided by the context of the research objectives. These aims determine the methodology that is best suited to collect the data. The main objectives includes:

- i. To examine the ethical justification for government-mandated encryption backdoors using philosophical theories.
- ii. To assess how encryption backdoors affect individual rights on a legal framework.

- iii. To evaluate the technical risks of implementing backdoors, such as weakening security
- iv. To analyze how governments can ethically balance national security interests with protecting digital rights and public trust.
- v. To review real-world examples of government attempts to implement backdoors, including industry and public responses, to assess ethical and societal impacts.

Research Questions

Based on the five research objectives, questions have been developed to guide the research even further. These questions provide more direct paths of explorations to investigate. The questions are designed to discover and fill gaps in knowledge and provide a baseline of understanding of ethics and government surveillance. The questions are the following:

RQ1: What are government backdoors and what are the risks of system integrity and user trust?

RQ2: How can ethical principles of utilitarianism, deontology, and other right-based ethical theories be applied to the debate over encryption backdoors?

RQ3: How do international legal frameworks address the tension between government surveillance and digital privacy?

RQ4: Should the protection of citizens from harm (e.g., terrorism) outweigh the right to digital privacy?

Data Collection Methodology

For this study, data were collected primarily through an extensive review of scholarly literature and credible academic sources. The data collection process involved identifying, retrieving, and analyzing existing research relevant to the ethics of government backdoors in

encryption systems. This method ensured that the study was grounded in established theoretical perspectives, current legal discussions, and ongoing policy debates within the fields of cybersecurity, ethics, and governance.

The primary sources of data were obtained through several government websites and academic and institutional databases. Google Scholar was used as a key search tool to locate peer-reviewed articles, theses, and books across political, ethical, and technological disciplines. Its broad coverage and filtering capabilities helped ensure that only credible and relevant sources were selected for analysis.

Additionally, the Marymount University Library Catalog and MULibrary Search served as critical tools for locating scholarly materials, including books, government documents, journal articles, and other media resources available both online and in print through the Reinsch Library. Librarian assistance, available through the university's online chat service, was also utilized to refine search strategies and verify the relevance of selected materials.

The data collection was limited primarily to publications from 2021 to 2025 to ensure the inclusion of current perspectives on technology and policy. However, two foundational works, *Consequentialism and Human Rights* by William J. Talbott (2013) and *The Debate on Privacy Protection: Should It Be Unlimited?* by Stephen J. Kobrin and Thomas Donaldson (1999), were intentionally included for their significance in understanding theoretical views.

Data Analysis Plan

Because this study is grounded in a qualitative research methodology, the data analysis relies primarily on thematic analysis to identify, interpret, and evaluate patterns within the collected literature. This approach is appropriate given the ethical and philosophical nature of the

research topic, which centers on understanding differing perspectives, moral frameworks, and policy arguments rather than producing numerical or statistical results.

The analysis process begins with close reading and annotation of all selected sources, focusing on recurring ethical arguments, legal justifications, and political positions regarding government backdoors in encryption systems. Each text is examined for key themes and concepts such as privacy vs. security, ethical justification of surveillance, government accountability, and public trust in digital systems. These themes are then coded and categorized into broader analytical groups to facilitate systematic comparison across multiple viewpoints.

During coding, data is organized into categories that align with the study's research questions and objectives. For example, discussions related to deontological ethics are coded separately from those emphasizing utilitarian or consequentialist reasoning. Similarly, legal or policy-based arguments are grouped distinctively from moral or philosophical discussions. This process helps identify both consensus and divergence among scholars, policymakers, and ethicists on the legitimacy and potential dangers of implementing government backdoors.

One limitation of this analytical method is the potential for subjectivity in theme identification and interpretation, as qualitative analysis depends heavily on the researcher's judgment. To address this, themes are cross-checked for consistency, and the findings are interpreted through established ethical frameworks and academic consensus wherever possible. Another limitation arises from relying solely on secondary data, which may not capture unpublished or classified government perspectives. This is mitigated by incorporating diverse sources, including government publications, peer-reviewed research, and reputable media analyses, to ensure a balanced and comprehensive view.

Trustworthiness

Ensuring the trustworthiness of this research is essential to demonstrate the credibility, validity, and reliability of its findings. Because this study employs a qualitative methodology, trustworthiness is established through transparent research practices, critical evaluation of sources, and consistent analytical procedures.

Together, the diverse professional expertise of the authors used within this research paper, spanning cybersecurity practice, ethical theory, applied machine learning, internet policy advocacy, and rights philosophy, provides a robust foundation for their arguments and thereby supports the trustworthiness of the literature base used within the study.

Credibility is achieved through the careful selection of reputable, peer-reviewed, and institutionally verified sources. Materials were drawn from scholarly databases such as Google Scholar, the Marymount Library catalog, and government or university-affiliated publications. The inclusion of both recent studies (2021–2025) and foundational ethical works (e.g., Talbott, 2013; Kobrin & Donaldson, 1999) ensures that the analysis reflects both current debates and enduring moral principles. Triangulation, drawing from ethics, law, and cybersecurity, further supports credibility by allowing cross-comparison of perspectives.

Validity is maintained by aligning the data analysis process with the study's research questions and theoretical frameworks. Ethical perspectives such as utilitarianism, deontology, and consequentialism guide interpretation, ensuring consistency and conceptual understanding.

Reliability is upheld through a systematic and transparent analytical process. All sources were reviewed and coded according to recurring themes such as *privacy versus security*, *ethical justification of surveillance*, and *public trust*. Consistent coding and interpretation across sources help minimize researcher bias and maintain logical consistency throughout the analysis.

Limitations to trustworthiness primarily arise from the use of secondary data and the interpretive nature of qualitative analysis. While direct government or classified perspectives are inaccessible, this limitation is addressed by incorporating diverse and credible sources. Potential bias is mitigated through balanced representation of opposing viewpoints and adherence to established ethical research standards.

Overall, the research's credibility, validity, and reliability are reinforced through careful source selection, theoretical grounding, and transparent methodology, ensuring findings that are dependable, balanced, and academically sound.

Ethical Considerations

This study adheres to established ethical standards for academic research as outlined by Marymount University's Institutional Review Board (IRB) and broader principles of academic integrity. Because the research is qualitative and relies exclusively on secondary data, no human participants were directly involved; therefore, issues of participant consent, confidentiality, or physical harm are not applicable. However, ethical diligence remains essential to ensure the responsible use and interpretation of all sources.

All materials used in this research were obtained from reputable and publicly accessible databases, including Google Scholar, government websites, and university libraries. Proper citation and attribution practices were strictly followed to respect intellectual property and avoid plagiarism. Each source was evaluated for accuracy, relevance, and credibility before inclusion to prevent the distribution of misleading or fabricated information.

The integrity of data collection and analysis was maintained through transparency in research methods and consistent adherence to the study's objectives. No data manipulation, selective omission, or alteration of findings occurred at any point during the process. Ethical

reasoning and scholarly honesty guided all interpretations, particularly in evaluating conflicting viewpoints on government surveillance and privacy ethics.

As this project did not involve direct data collection from individuals or organizations, IRB approval was not required. Nonetheless, the study was conducted under the ethical expectations of Marymount University's capstone research policies, emphasizing honesty, respect for intellectual contributions, and accuracy in reporting findings.

Overall, this research upholds the principles of ethical scholarship by ensuring transparency, protecting the integrity of data, and maintaining respect for the intellectual work of others while exploring the complex ethical implications of government backdoors in encryption systems.

Summary

This qualitative research study investigates the ethics of government-mandated encryption backdoors through an extensive literature review approach. The methodology is grounded in qualitative research principles that prioritize gathering diverse perspectives, experiences, and philosophical viewpoints rather than numerical data. The study is guided by five core objectives examining ethical justifications, legal frameworks, technical risks, and real-world impacts of encryption backdoors, with four research questions exploring government backdoor risks, ethical principles (utilitarianism, deontology), international legal tensions, and the balance between security and privacy.

Primary data sources include peer-reviewed scholarly literature accessed through Google Scholar, Marymount University Library databases, and government publications, with research focusing on materials published between 2021-2025 to capture current perspectives alongside selective inclusion of foundational ethical texts from earlier periods. The study employs thematic

analysis to identify patterns across collected literature, with sources systematically coded according to recurring themes such as privacy versus security, ethical justifications for surveillance, and public trust. Arguments are categorized by ethical framework (deontological, utilitarian, consequentialist) and discipline (legal, philosophical, policy-based) to enable comparative analysis.

Trustworthiness is established through careful source selection from reputable databases and triangulation across ethics, law, and cybersecurity disciplines. Credibility is maintained by aligning analysis with research questions and established ethical frameworks, while reliability is ensured through systematic, transparent coding procedures. The study adheres to academic integrity standards, using only publicly accessible secondary sources with proper attribution. No IRB approval was required as no human participants were involved in this secondary data analysis.

Chapter 4: Data Analysis

Overview

This chapter analyzes the data collected through qualitative research to address the ethical, legal, and technical implications of government-mandated encryption backdoors. The purpose of this analysis is to interpret the data in relation to the study's objectives and research questions, providing a comprehensive understanding of how backdoors influence privacy, security, and ethical governance.

The research was guided by five questions: What are government backdoors and what risks do they pose to system integrity and user trust? How can ethical theories such as utilitarianism, deontology, and rights-based ethics be applied to the debate? How do international legal frameworks address the tension between surveillance and privacy? Should national security outweigh the right to digital privacy? and Is it ethically justifiable for governments to mandate encryption backdoors for national security purposes? These questions form the foundation for the organization and interpretation of data throughout this chapter.

The study employed a qualitative research design, relying on secondary data gathered through scholarly articles, government publications, and institutional reports. Thematic analysis was used to identify recurring patterns and arguments related to encryption backdoors. Data were grouped into four major themes: technical and security risks, ethical evaluation frameworks, legal and regulatory patterns, and public sentiment. This approach enabled a comprehensive examination across ethical, technological, and societal domains, aligning with the interdisciplinary nature of the topic.

For clarity, key terms used throughout the analysis include: encryption backdoors, referring to intentional access points in encrypted systems that allow government or law

enforcement entry (Paula Bernardi & Celia Richardson, 2025). Digital privacy, the right of individuals to control their personal data and communications (Rebecca Hamlin, 2025). Ethics, the study of moral principles guiding right and wrong actions (Peter Singer, 2025). And National security, the protection of a nation's safety and interests against internal or external threats (LegalClarity, 2025). Understanding these terms ensures that readers from diverse backgrounds can follow the discussion consistently.

This chapter is structured into four main parts. The Data Results section presents the refined findings from the literature without interpretation, using tables and figures to summarize trends. The Data Analysis section interprets these results in relation to the research questions and theoretical frameworks. The Summary consolidates the main insights and highlights any limitations in the analysis. Together, these components offer a thorough and balanced exploration of the ethics and implications of government backdoors in encryption systems.

Data Results

The research collected in Chapter 2 resulted in extensive material from multiple disciplines, requiring systematic refinement to ensure clarity and relevance. The data cleansing process began by eliminating redundant information where multiple sources presented identical factual claims without adding new perspectives. For instance, several sources defined encryption backdoors using nearly identical language; only the most comprehensive and authoritative definitions from Bernardi and Richardson (2025) were retained for analysis, while repetitive definitions were excluded.

Sources were evaluated for modern relevance, with materials published between 2021 and 2025 prioritized to capture current technological and policy contexts. However, foundational ethical works by Talbott (2013) and Kobrin and Donaldson (1999) were intentionally retained

despite falling outside this timeframe due to their enduring theoretical significance for rights-based and consequentialist frameworks.

Data was further refined by identifying the best contribution of each source to avoid duplication. When multiple sources discussed the same case study, such as the FBI-Apple encryption dispute, only those offering distinct analytical perspectives or new factual information were retained. Sources presenting overlapping arguments were compared, with the most comprehensive or well-cited version selected for detailed analysis. This process ensured that the dataset represented a diversity of perspective rather than repetition of similar viewpoints.

After this systematic cleansing process, all literature gathered in Chapter 2 was removed of any data that were repetitive, secondary, or lacked verifiable or theoretical depth. Articles that only restated existing knowledge without contributing new ethical or technical insights were removed. Priority was given to peer-reviewed studies, government publications, and research papers that provided verifiable evidence or theoretical analysis related directly to encryption backdoors, privacy, and ethics. Outdated or biased materials, such as opinion-based commentaries, were excluded to maintain data reliability. The final dataset consisted of twelve core sources categorized across ethical, technical, legal, and societal frameworks, ensuring that the results reflected balanced and diverse perspectives.

Table 1: Post-Data Cleansing Source Categories

| Category/Theme | Number of Sources |
|-------------------------------|-------------------|
| Technical and Security Risks | 4 |
| Ethical Evaluation Frameworks | 3 |
| Legal and Regulatory Patterns | 3 |
| Societal/Public Perception | 2 |

After cleansing, the refined literature was grouped into four major themes based on recurring discussions and points of consensus identified across the reviewed sources. The themes include Technical and Security Risks of Backdoors, Ethical Evaluation Frameworks, Legal and Regulatory Patterns, and Public Sentiment and Societal Perceptions.

Across all data groups, a unified pattern is shown, the pursuit of national security through encryption backdoors introduces ethical, legal, and social costs that consistently outweigh the perceived benefits. The literature collectively illustrates that while governments frame surveillance as protective, the resulting consequences, loss of privacy, weakened system security, and declining public trust, reveal an enduring global tension between safety and digital rights.

Government Backdoors and their Risks to System Integrity and User Trust

The data revealed that government backdoors are intentional design features that provide authorized third-party access to encrypted data. Studies by Bernardi & Richardson (2025) and Forno (2025) consistently highlight how such access points compromise digital security and public trust. From a technical perspective, backdoors create inherent vulnerabilities, making encryption systems more susceptible to cyberattacks.

Comparatively, these findings align with the Internet Society's argument that "no system can remain secure once exceptional access exists," supporting the broader cybersecurity consensus that security cannot coexist with selective accessibility. The Apple, FBI and U.K. Investigatory Powers cases exemplify how corporate refusal to weaken encryption is rooted not in deliberately defying, but in preserving user trust and digital integrity.

The implication is that the government's attempt to achieve total security contradicts systemic insecurity. Users' confidence in technology erodes when confidentiality is uncertain, illustrating that security and trust are mutually reinforcing, not conflicting. This relationship is

crucial to ethical policymaking in cybersecurity, a secure but distrusted system ultimately undermines public cooperation and compliance.

Technical and Security Risks of Backdoors

Data from Bernardi & Richardson (2025) and Forno (2025) consistently indicated that government-mandated encryption backdoors weaken cybersecurity by creating exploitable vulnerabilities. Case studies such as Apple’s refusal to develop a “Clipper Chip” equivalent revealed a universal pattern: while backdoors aim to increase surveillance capability, they simultaneously decrease public trust and system integrity.

Table 2: Summary of Technical Findings

| Primary Findings | Focus | Source |
|--|---------------------------|------------------------------|
| Backdoors create exploitable weaknesses and undermine encryption integrity | Technical vulnerabilities | Bernardi & Richardson (2025) |
| Corporate resistance is linked to preserving user privacy and system trust | Real-world case studies | Forno (2025) |

Ethical Principles Applied

Analysis of the ethical frameworks revealed fundamental differences in moral reasoning. Utilitarian approaches (Lawcenta, 2024) suggest that government surveillance may be justified if the benefits, such as crime prevention or national protection, outweigh privacy harms. However, deontological perspectives (Prabhumoye et al., 2021) reject this consequentialist reasoning, emphasizing that privacy and autonomy are moral duties, not negotiable goods. Talbott’s (2013) consequentialist model bridges these views, arguing that human rights-based systems yield the best long-term societal outcomes, even when short-term sacrifices appear justified.

Comparing these frameworks shows a recurring ethical tension: utilitarianism prioritizes societal welfare, while deontology and rights-based ethics prioritize individual integrity. Applied to backdoors, utilitarian ethics might condone limited intrusion for security purposes, but both deontological and rights-based reasoning find such actions morally impermissible because they treat citizens as means to an end.

The synthesis of these frameworks suggests that sustainable digital ethics must uphold rights as a moral baseline, not as a variable within cost–benefit calculations. Government access to private data, even under noble pretenses, therefore violates foundational ethical principles and long-term public trust.

Ethical Evaluation Frameworks

The reviewed ethical data, drawn from Lawcenta (2024), Prabhumoye et al. (2021), and Talbott (2013), highlighted contrasting moral standpoints. Utilitarian perspectives allow for limited privacy trade-offs if the societal benefit outweighs harm, while deontological ethics reject surveillance that treats users merely as means to an end. Consequentialist ethics focus on long-term trust and the moral sustainability of surveillance policies.

Table 3: Comparison of Ethical Framework Outcomes

| Ethical Framework | Moral Position on Backdoors | Common Justification or Concern |
|-------------------|-----------------------------|--|
| Utilitarianism | Conditional acceptance | Balances harm vs. benefit. Allows intrusion for security |
| Deontology | Rejection | Violated autonomy and informed consent |
| Consequentialism | Cautious opposition | Warns of long-term trust erosion and |

| | | |
|--|--|----------------|
| | | systemic abuse |
|--|--|----------------|

Existing Legal Frameworks on Government Surveillance and Digital Privacy

Legal analyses by GovFacts (2025) and Broadbent (2024) show that both the U.S. and U.K. have expanded government surveillance powers under laws such as the USA PATRIOT Act and the Investigatory Powers Amendment Act (2024). While these laws aim to enhance national security, both countries face criticism for vague oversight mechanisms and inconsistent privacy protections.

Comparatively, the data reveal a significant legal imbalance, technological advancement outpaces legislative reform. Courts in both jurisdictions struggle to apply older constitutional and statutory frameworks to modern digital surveillance. For instance, *Carpenter v. United States* (2018) extended Fourth Amendment protections to digital data, but it remains unclear how these rights apply to encryption backdoors (GovFacts 2025). Similarly, the U.K.’s new amendment allows the government to delay or veto security updates, highlighting a legal structure that prioritizes access over autonomy (Broadbent 2024).

The implication is a growing legal-ethical gap, where laws enable surveillance without proportionate checks or transparency. This gap underscores the need for an updated digital rights law framework that integrates both privacy protection and legitimate state interests under clear, enforceable boundaries.

Legal and Regulatory Patterns

Data from GovFacts (2025) and Broadbent (2024) demonstrate how government surveillance powers have expanded under laws such as the USA PATRIOT Act and the U.K.’s Investigatory Powers Amendment Act (2024). Despite the stated goals of public safety, both legal frameworks suffer from insufficient oversight and lack clear proportionality standards.

Table 4: Comparative Overview of Legal Trends

| Country | Key Legislation | Surveillance Scope | Oversight Mechanism | Ethical Concern |
|----------------|---|---|----------------------------|---|
| United States | PATRIOT Act, FISA Section 702 | Broad access to encrypted data | Secret court review (FISC) | Weak transparency, risk of abuse |
| United Kingdom | Investigatory Powers Act 2016 & 2024 Amendments | Mandatory reporting of encryption changes | Ministerial approval | Potential violation of privacy rights and innovation slowdown |

Citizen Protection versus Digital Privacy

The data suggest that while national security is a legitimate government function, the notion that it should outweigh individual privacy is ethically unstable. McClain et al. (2023) found that 71% of citizens distrust government data collection, even when justified as protective. This aligns with Kobrin & Donaldson's (1999) communitarian argument that privacy rights may be limited for societal welfare but must remain proportionate and transparent.

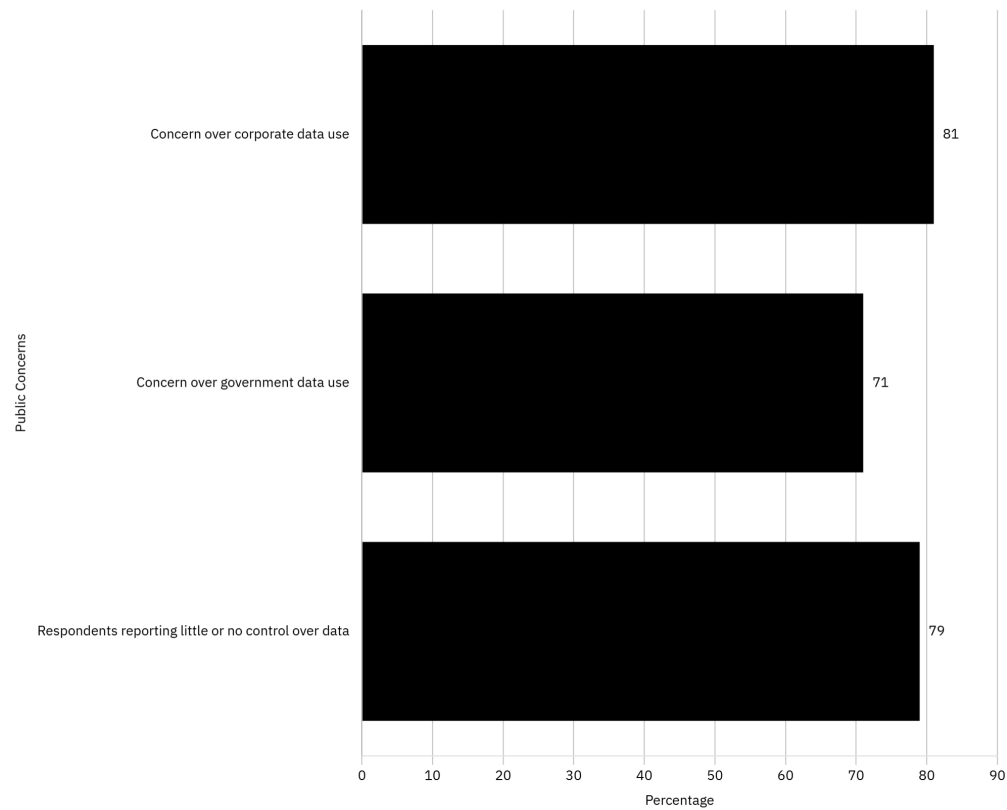
When compared with Etzioni's "minimal intrusion" principle, which supports privacy limitations only when no less invasive alternative exists, government backdoors fail the ethical test. They represent maximal intrusion by default, granting continuous, system-level access rather than case-specific oversight. Furthermore, observed evidence indicates that broad surveillance rarely prevents crime but consistently diminishes public trust and democratic accountability.

Therefore, the analysis concludes that security and privacy are not mutually exclusive, they must coexist within ethical and procedural limits. Sacrificing privacy in the name of security may produce temporary reassurance but leads to long-term reduction of civil liberties and institutional legitimacy.

Public Sentiment and Societal Perceptions

Survey results summarized by McClain et al. (2023) revealed widespread skepticism toward both government and corporate data practices. Over 70% of participants expressed concern about data misuse, and the majority reported feeling powerless over how their information is collected or shared. These results align with findings from Kobrin & Donaldson (1999) and Scott & Ó Floinn (2024), showing that citizens favor transparency and accountability over unrestricted surveillance.

Figure 1: Public Concern Over Data Privacy



Ethical Justifiability of Government Backdoors

Synthesizing the findings across all themes, there is limited ethical justification for government-mandated backdoors. From an ethical perspective, such mandates violate autonomy and informed consent (deontology), fail cost–benefit proportionality (utilitarianism), and undermine human rights (rights-based ethics). From a legal and technical standpoint, they weaken cybersecurity infrastructures, produce systemic vulnerabilities, and foster public distrust.

Comparatively, across all reviewed sources, no data indicated a successful or risk-free implementation of government backdoors. Even proponents of limited surveillance acknowledge the impossibility of creating an access mechanism that benefits only authorized actors. Thus, the ethical justification collapses when evaluated against both moral theory and empirical evidence.

The broader implication is that ethical cybersecurity governance requires transparency, necessity, and proportionality. Policies that prioritize surveillance without addressing these principles not only fail ethical inspection but risk delegitimizing democratic institutions that rely on public consent and digital trust.

Summary

While this analysis provides a comprehensive interpretation of the data, several limitations should be acknowledged. First, the study relies exclusively on secondary data, which restricts firsthand perspectives from policymakers or government agencies. Second, because much of the data is qualitative, the analysis reflects interpretive reasoning rather than quantifiable measurement. Additionally, the evolving nature of cybersecurity legislation means that new laws or policies may shift the ethical and legal landscape beyond the scope of this study. Finally, the lack of access to classified or restricted government documentation limits full evaluation of state-level intentions or safeguards.

Despite these limitations, triangulation across ethical, legal, technical, and social domains provides a robust foundation for evaluating the moral legitimacy of encryption backdoors and their impact on privacy, trust, and governance.

The findings from this study reveal a consistent conflict between the pursuit of national security and the protection of individual digital rights. Across all analyzed literature, government-mandated encryption backdoors were shown to generate more ethical, legal, and technical concerns than practical benefits. Although such measures are justified as tools for crime prevention and public safety, the data indicate that they fundamentally weaken digital security and public trust.

From a technical standpoint, studies by Bernardi & Richardson (2025) and Forno (2025) confirmed that backdoors introduce exploitable vulnerabilities that compromise system integrity and user privacy. This recurring pattern demonstrates that exceptional access, even when limited to authorized actors, cannot exist without reducing overall cybersecurity.

Ethically, contrasting frameworks provided valuable insight into the moral dimensions of surveillance. Utilitarian models, as presented by Lawcenta (2024), conditionally support backdoors when societal benefit outweighs harm. However, deontological and rights-based perspectives (Prabhumoye et al., 2021; Talbott, 2013) reject these measures outright, emphasizing that privacy and autonomy are moral obligations, not negotiable interests. The convergence of these viewpoints suggests that the ethical justification for government backdoors cannot be sustained without violating fundamental moral principles.

Legal analyses by GovFacts (2025) and Broadbent (2024) revealed similar inconsistencies in both the United States and United Kingdom, where surveillance laws continue

to evolve faster than oversight mechanisms. This imbalance reinforces a widening gap between technological innovation and regulatory accountability.

Finally, public perception data from McClain et al. (2023) demonstrated widespread distrust toward government data collection and a growing demand for transparency, accountability, and privacy protection. The ethical, technical, and societal patterns all point toward the same conclusion, government backdoors, while framed as instruments of protection, create greater long-term harm by undermining the integrity of digital systems and dismantling civil trust.

Overall, the interpretation of the data establishes that encryption backdoors are ethically indefensible and practically unsustainable. They illustrate the need for cybersecurity policies that integrate privacy as a foundational right and ethical standard rather than a negotiable trade-off. These insights form the groundwork for the concluding chapter, which discuss the broader implications, conclusions, and recommendations derived from this study.

Chapter 5: Discussion, Recommendations, & Conclusions

Summary of the Results

This study examined the ethical, legal, technical, and societal implications of government-mandated encryption backdoors. The results were organized around the research questions and reflect the patterns found across the twelve core sources analyzed after data refinement.

Regarding the first research question, the findings showed that government backdoors are intentional access mechanisms that allow authorized third parties to bypass encryption. Data from technical sources consistently demonstrated that such access points introduce security vulnerabilities that weaken overall system integrity. Case studies, including Apple's refusal to create government-requested access tools, further indicated that backdoors reduce user trust and increase the likelihood of system exploitation.

For the second research question on ethical theories, the results indicated clear differences across moral frameworks. Utilitarian sources allowed for the conditional acceptance of backdoors if societal benefits outweigh harms. In contrast, deontological sources uniformly reject backdoors on the basis that they violate autonomy and informed consent. Consequentialist sources expressed concern about long-term impacts on public trust and institutional legitimacy, even in cases where short-term gains might be claimed.

With respect to legal frameworks in the United States and United Kingdom, the results showed ongoing expansion of government surveillance authority. U.S. laws such as the USA PATRIOT Act and FISA Section 702 authorize broad access to digital data, supported by limited oversight mechanisms. In the U.K., amendments to the Investigatory Powers Act give the government authority to delay or block encryption upgrades. Across both jurisdictions, the data

reflected inadequate transparency and oversight, along with legal vagueness in applying older privacy protections to modern encryption.

Results related to national security and the right to privacy showed that public opinion trends heavily toward distrust of both government and corporate data practices. Survey data indicated that majorities of citizens feel they lack control over their personal information and are concerned about potential misuse. These findings align with ethical arguments suggesting that privacy intrusions require proportionality, minimal interference, and clear justification.

Finally, results addressing the overall ethical justifiability of government-mandated backdoors showed no evidence of a successful model in which backdoors protected security without compromising system integrity or individual rights. Across all sources, the data repeatedly demonstrated that backdoors introduce technical risks, reduce public trust, and are subject to legal and ethical limitations that restrict their viability as surveillance tools.

Interpretation of Findings

The findings of this study largely align with the existing body of literature, demonstrating a broad consensus that encryption backdoors introduce more risks than benefits, both technically and ethically. The results reinforce the conclusions of Bernardi & Richardson (2025) and Forno (2025), who argue that backdoors inherently weaken encryption by creating points of vulnerability. The observed agreement suggests a stable and widely accepted understanding across the cybersecurity field that exceptional access cannot coexist with uncompromised system security. No reviewed source provided verifiable support for a technically viable method of implementing backdoors without introducing new attack surfaces. Which in return reflects a continued agreement in the literature that the security drawbacks are structural rather than situational.

Ethically, the findings reflected clear distinctions among utilitarian, deontological, and consequentialist perspectives, consistent with the arguments presented in the literature. The utilitarian framework, as outlined by Lawcenta (2024), offers conditional justification for backdoors only if the societal benefits outweigh privacy harms. However, the study's findings suggest that such benefits are speculative, while the harms, particularly the weakening of system integrity and potential for misuse, are well documented. This discrepancy indicates that, in practice, utilitarian justification is difficult to achieve, reinforcing the criticisms of privacy advocates who argue that security requirements rarely produce proportional benefits.

Deontological perspectives from Prabhumoye et al. (2021) were strongly reflected in the results, particularly regarding violations of autonomy and consent. Backdoors treat users as means to state ends, an ethical breach that persists regardless of intended government purpose. The findings align with deontological literature in showing that the moral objections to backdoors are not dependent on outcomes but on incompatibilities with user rights and digital autonomy.

Consequentialist reasoning, as described by Talbott (2013), provided a useful interpretive lens for understanding long-term implications. The results show that even if backdoors could produce short-term investigative benefits, the broader institutional consequences, loss of trust, normalization of surveillance, and diminished technological integrity, outweigh such benefits. This interpretation suggests that the underlying mechanism driving opposition is not merely fear of immediate misuse but recognition of the systemic effects that undermine the stability of the digital environments and democratic institutions.

Legally, the findings underscore a recurring pattern in the literature, the expansion of surveillance powers outpaces the development of adequate oversight frameworks. GovFacts

(2025) and Broadbent (2024) both highlight that while governments justify surveillance expansion through safety narratives, corresponding accountability structures remain limited or vague. The findings reflect this tension, indicating that legal mechanisms often lag behind technological developments, creating gaps in which backdoors can be implemented without sufficient safeguards. This interpretation points to an underlying governance mechanism in which technological capability advances faster than legal or ethical constraints.

Public perception results further deepen the interpretation of the ethical argument. McClain et al. (2023) report widespread public distrust of data practices, and these findings align with the study's conclusion that such distrust is justified by the technical risks and lack of transparency associated with backdoors. This suggests a feedback loop. Government pursuit of exceptional access reduces trust, and reduced trust diminishes the legitimacy and effectiveness of government interventions. The consistency between public sentiment and scholarly concerns strengthens the interpretation that backdoors pose not only technical and ethical risks but also social and democratic risks.

Overall, the findings support the prevailing argument in the literature that encryption backdoors are incompatible with strong digital privacy, democratic accountability, and long-term cybersecurity. While theoretical justifications exist in limited ethical frameworks, the practical implications, observed patterns, and underlying mechanisms consistently point toward substantial risk with insufficient evidence of proportional benefits. The interpretation of these findings suggests that the ethical and technical debates surrounding backdoors are driven not only by abstract moral principles but also by real-world consequences inherent to weakening encryption systems.

Limitations of Study

This study is subject to several limitations that should be considered when interpreting the findings. First, the research relied solely on secondary sources, which restricted the analysis to information already published in academic literature, government documents, and organizational reports. As a result, perspectives from policymakers, industry engineers, or law-enforcement personnel directly involved in encryption debates may be underrepresented.

A second limitation involves potential bias within the available literature. Most scholarly and technical publications emphasize the risks associated with backdoors, creating an imbalance in which pro-backdoor arguments are less prevalent or supported by fewer empirical studies. While the research attempted to incorporate multiple viewpoints, the dominance of critical perspectives may influence the overall interpretation.

The study's qualitative approach also limits generalizability. The selected sources, although diverse, do not represent a statistically significant sample, and public opinion findings were drawn from a small number of surveys that may not reflect demographic or regional variation. Additionally, cybersecurity technologies and legal frameworks evolve rapidly, meaning that conclusions based on current literature may shift as new developments emerge.

Future research could address these limitations through primary data collection, including expert interviews or broader public surveys, as well as comparative international studies. Technical investigations into alternative access models or emerging encryption technologies could also offer deeper insight into whether secure and ethically acceptable forms of government access are feasible.

Recommendations

Based on the findings of this study, several recommendations can be made for policymakers, cybersecurity practitioners, and researchers. These recommendations emphasize realistic and sustainable actions supported by the evidence gathered.

Policymakers should avoid implementing mandated encryption backdoors due to the demonstrated security vulnerabilities and ethical concerns identified in the literature. Instead, governments should prioritize developing clear, transparent legal frameworks that balance national security needs with the protection of individual privacy rights. Strengthening oversight mechanisms, such as independent review boards, audit requirements, and public reporting, can improve accountability and reduce the risk of misuse. Policymakers should also invest in alternative investigative strategies, including targeted warrants, metadata analysis, and improved inter-agency cooperation, which do not weaken encryption.

Technology companies and cybersecurity professionals should continue to implement strong, end-to-end encryption and resist pressure to introduce backdoors or “exceptional access” pathways. The results suggest that maintaining robust encryption is essential for preserving user trust and preventing system exploitation. Practitioners should also emphasize secure system design, including routine vulnerability assessments and transparent communication with users about privacy protections. Collaboration with government agencies on lawful access procedures should focus on methods that do not undermine encryption, such as secure device-based extraction when legally authorized.

Advocacy groups should continue educating the public about the risks associated with encryption backdoors and promote privacy-preserving digital practices. The findings indicate significant public concern regarding government access to data; therefore, outreach and policy

engagement efforts can help ensure that public voices remain a central part of surveillance policy debates. Organizations may also serve as watchdogs by monitoring legislative developments and raising awareness when policies threaten privacy or cybersecurity.

Further research is needed to explore technical alternatives to backdoors, such as privacy-preserving access models or advanced digital forensics tools. Studies incorporating expert interviews, simulations, or case analyses could provide deeper insight into practical solutions that meet investigative needs without compromising security. Additional large-scale surveys would also help capture diverse public perspectives, contributing to a more comprehensive understanding of societal attitudes toward encryption and government surveillance.

Collectively, these recommendations aim to support secure, ethical, and sustainable approaches to digital privacy and national security, ensuring that future policy decisions are grounded in evidence rather than theoretical assumptions.

Conclusion

This study contributes to the ongoing discourse surrounding encryption backdoors by synthesizing ethical, legal, and technical perspectives to reveal the substantial risks associated with government-mandated access to encrypted systems. The findings reinforce the importance of maintaining strong encryption as a foundation of digital security and highlight how backdoors undermine both user trust and system integrity. By examining the issue through multiple ethical frameworks and across differing legal environments, the research expands current understanding of why backdoors remain a contentious and largely unviable solution within the cybersecurity field.

The significance of this study lies in its ability to bring together diverse strands of literature and present a comprehensive view of the implications of exceptional access. In doing so, it advances scholarly knowledge by clarifying the underlying mechanisms that make backdoors ethically problematic, technically unsound, and legally complex. The research also underscores the broader societal implications, particularly regarding public trust, privacy expectations, and democratic accountability.

Future research should continue exploring alternative investigative methods that do not compromise encryption, including emerging forensic tools and privacy-preserving access models. Additional studies involving expert interviews, cross-national comparisons, and large-scale public surveys would further deepen the understanding of how encryption policies are shaped and perceived.

Overall, this study demonstrates that while the tension between national security and individual privacy continues to evolve, weakening encryption through mandated backdoors presents significant and persistent risks. The research journey underscores the need for solutions that uphold both security and ethical integrity, supporting a digital future built on trust, transparency, and technological resilience.

References

- Bernardi, P., Richardson, C., & Internet Society. (2025, May 2). *What is an Encryption Backdoor?*
<https://www.internetsociety.org/blog/2025/05/what-is-an-encryption-backdoor/>
- Broadbent, M., & CSIS. (2024, May 20). *A New Investigatory Powers Act in the United Kingdom Enhances Government Surveillance Powers.*
<https://www.csis.org/analysis/new-investigatory-powers-act-united-kingdom-enhances-government-surveillance-powers>
- Forno, R., & UMBC. (2025, May 16). *Governments Continue Losing Efforts to Gain Backdoor Access to Secure Communications.*
<https://umbc.edu/stories/governments-continue-losing-efforts-to-gain-backdoor-access-to-secure-communications/>
- GovFacts. (2025, August 10). *Government Surveillance vs. Personal Privacy.*
<https://govfacts.org/explainer/government-surveillance-vs-personal-privacy/>
- Hamlin, R. (2025, September 13). *Civil rights | Definition, Types, Activists, History, & Facts.* Britannica. Retrieved September 28, 2025, from
<https://www.britannica.com/topic/civil-rights>
- Kobrin, S. J., Donaldson, T., & Knowledge at Wharton. (1999, May 24). *The Debate on Privacy Protection: Should it be Unlimited?*
<https://knowledge.wharton.upenn.edu/article/the-debate-on-privacy-protection-should-it-be-unlimited/>
- Lawcenta Team. (2024, April 2). *Applying Utilitarian Ethics to Privacy Laws for Public Benefit.*
<https://lawcenta.com/applying-utilitarian-ethics-to-privacy-laws/>

LegalClarity. (2025, August 26). *What Does National Security Mean? A Modern Definition*.

<https://legalclarity.org/what-does-national-security-mean-a-modern-definition/>

McClain, C., Faverio, M., Anderson, M., & Park, E. (2023, October 18). *Views of data privacy risks, personal data and digital privacy laws*. Pew Research Center.

[https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-d
ata-and-digital-privacy-laws/](https://www.pewresearch.org/internet/2023/10/18/views-of-data-privacy-risks-personal-data-and-digital-privacy-laws/)

Prabhumoye, S., Boldt, B., Salakhutdinov, R., Black, A. W., & Carnegie Mellon University.

(2021, April 12). *Case Study: Deontological Ethics in NLP*.

<https://arxiv.org/pdf/2010.04658>

Scott, P. F., & Floinn, M. O. (2024, December 26). Technical Backdoors and Legal Backdoors: Regulating Encryption in the UK. *King's Law Journal*, 35(3), 441-476.

<https://www.tandfonline.com/doi/full/10.1080/09615768.2024.2444720#d1e99>

Singer, P. (2025, August 19). *Ethics | Definition, History, Examples, Types, Philosophy, & Facts*.

Britannica. Retrieved September 28, 2025, from

<https://www.britannica.com/topic/ethics-philosophy>

SURVEILLANCE | English meaning - Cambridge Dictionary. (2025, September 24). Cambridge Dictionary. Retrieved September 28, 2025, from

https://dictionary.cambridge.org/dictionary/english/surveillance#google_vignette

Talbott, W. J. (2013, November 4). Consequentialism and Human Rights. *Philosophy Compass*,

8(11), 1030-1040. <https://compass.onlinelibrary.wiley.com/doi/10.1111/phc3.12084>

Yin, R. K. (2015). *Qualitative Research from Start to Finish*. Guilford Publications.

<https://eli.johogo.com/Class/Qualitative%20Research.pdf>