Automated Databases and Hand-Typed Queries: Section 702 and Artificial Intelligence

Nakul Sharma[*]

What happens when the United States' most important foreign intelligence program meets modern artificial intelligence? This Note explores this question and posits that human observability is a critical predicate for any privacy harms that result from automated searches of Section 702 intelligence data. Using a large-language-model-enhanced search engine as a stand-in for redacted NSA and CIA systems, this Note reconstructs how automated querying could operate inside the procedural framework created by Section 702 of the Foreign Intelligence Surveillance Act. It then reviews the legal authorities that undergird Section 702 surveillance. This Note then combines these technical and legal analyses and applies them to recent, court-approved procedural changes to Section 702 surveillance that are likely real-world examples of artificial intelligence being used by the American Intelligence Community. This Note concludes by proposing human observability as a threshold question for whether automated surveillance systems warrant higher legal scrutiny. Systems that render otherwise protected information observable warrant higher legal scrutiny, whereas systems that do not do so do not warrant higher scrutiny.

* Articles Editor, Volume 104, *Texas Law Review*; J.D. Candidate, Class of 2026, The University of Texas School of Law. Thank you to my parents and sister for their immeasurable patience and support. Thank you also to Director Adam Klein, without whom this Note would not have been possible. And finally, thank you to the editors at the *Texas Law Review*. I would especially like to thank Notes Editors Francesca Chu and Piper Christenson, Articles Editor Laura Zhang, and Managing Editor Natalie Robinson for their thoughtful comments and kind-hearted patience.

INTRODUCTION 1351
I. THE INTERNET AND THE TECHNOLOGY OF ELECTRONIC SURVEILLANCE 1353
A. Networked Surveillance and the Internet 1354
B. Googling for Foreign Intelligence: Information Retrieval and Electronic Surveillance 1355
1. A (Very) Brief Primer on Automation and Large Language Models 1355
2. Search Engines as a Proxy for Section 702 Querying 1357
II. AN OVERVIEW OF SECTION 702 1359
A. Executive Order 12333 and Traditional FISA 1360
B. Section 702: A Procedural Scheme 1363
1. Targeting Procedures 1364
2. Minimization and Querying Procedures 1365
III. SECTION 702 SURVEILLANCE AND THE FOURTH AMENDMENT 1367
A. Incidental Collection and the Fourth Amendment 1368
B. Post-Collection Querying and the Fourth Amendment 1370
1. An Anti-Programmatic Approach to Reasonableness 1370
2. Reasonableness, the Totality of Circumstances, and Querying 1372
3. Comparing the Second Circuit and FISC's Approaches 1374
IV. NEW TECH, OLD RULES? 1375
A. Section 702 and Automated Processing 1375
1. 2023 NSA Automated Processing Procedures and FISC Approval 1375
2. 2024 CIA Automated Processing Tool and FISC Approval 1378
B. Schrödinger's Robot: Automating Fourth Amendment Reasonableness 1379
1. Analysts in the Loop 1380
2. Is Observation All You Need? 1381
CONCLUSION 1384

Introduction

Section 702 of the Foreign Intelligence Surveillance Act[1] is, by many accounts, the most important surveillance authority the United States has.[2] The "crown jewel of America's intelligence gathering capabilities," Section 702 surveillance has yielded myriad achievements.[3] It has helped foil terrorist plots, catch spies at home and abroad, and document atrocities in war-torn countries like Ukraine.[4]

Section 702's remarkable effectiveness arises out of the United States' central place in global information networks. Almost everyone's online data—whether American or not—are likely to pass through U.S. communications infrastructure.[5] Section 702 provides the U.S. government with the legal authority to tap into this fount of foreign intelligence information while also instituting procedural safeguards intended to protect Americans' privacy interests at home.[6]

These safeguards have often failed to garner public trust. Leaks and oversight reports have regularly created media firestorms around Section 702.[7] Section 702 draws further criticism from its place within the broader FISA surveillance regime. Section 702 and its associated amendments are the only FISA authorities that have a sunset provision.[8] And excesses from other, unrelated FISA authorities can and have come to bear on congressional debates on Section 702 renewal.[9]

Congress has used prior reauthorization votes to address such concerns around trust and privacy.[10] As this Note goes to print, Section 702 is again

---

1. 50 U.S.C. § 1881a.

2. *E.g.*, PRESIDENT'S INTEL. ADVISORY BD. & INTEL. OVERSIGHT BD., REVIEW OF FISA SECTION 702 AND RECOMMENDATIONS FOR REAUTHORIZATION 3 (2023).

3. 170 CONG. REC. S2760 (daily ed. Apr. 16, 2024) (statement of Sen. John Cornyn).

4. *Id.*; *see also, e.g.*, Charlie Savage & Julian E. Barnes, *U.S. Says Wiretap Program Thwarted Attack on 2024 Taylor Swift Concert*, N.Y. TIMES (Apr. 9, 2026), https://www.nytimes.com/2026/04/09/us/politics/section-702-surveillance-fisa.html [https://perma.cc/5A49-4TFH] (reporting on recent, government-provided examples of Section 702-based security successes).

5. *See infra* subpart I(A).

6. *See infra* Part II.

7. Charlie Savage, *Congress's Renewed Clash Over a Major Surveillance Law, Explained*, N.Y. TIMES (Mar. 19, 2026), https://www.nytimes.com/article/section-702-surveillance-law.html [https://perma.cc/CN4Y-YQGL].

8. ANDREAS KUERSTEN, CONG. RSCH. SERV., R48592.2, FISA SECTION 702 AND THE 2024 REFORMING INTELLIGENCE AND SECURING AMERICA ACT 1 (2025).

9. *See, e.g.*, Patrick G. Eddington, *Trump and FISA: A Fact Check*, CATO INST. (Apr. 11, 2024), https://www.cato.org/commentary/trump-fisa-fact-check [https://perma.cc/W473-KSBF] (noting how an improper use of traditional FISA surveillance affected arguments on Section 702 renewal).

10. For example, in 2018 Congress amended Section 702 to put guardrails around controversial "abouts" collection and subsequently prohibited its use under Section 702 in 2024. *Compare* 50 U.S.C. § 1881a(b)(5) (2018), *with* Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, § 22, 138 Stat. 892 (2024) (codified at 50 U.S.C. § 1881a(b)(5)). In its 2024 reauthorization, Congress also limited FBI access to Section 702 data in response to the agency's

up for reauthorization.[11] Congress has never let Section 702 lapse, and—despite increasingly tense rhetoric and worryingly last-minute reauthorizations—Congress is unlikely to deviate from this trend.[12]

However, Congress's current reauthorization debate has failed to keep up with today's changing technological environment. One of the most popular proposed reforms would impose a warrant requirement on querying Section 702 surveillance information for U.S. persons' information.[13] Whatever the merits of such a reform may—or may not—be, it largely addresses concerns that date back more than a decade at least.[14] Meanwhile, intelligence agencies likely have been using artificial intelligence-based tools to conduct Section 702 surveillance for the last few years at least.[15]

This use has rapidly accelerated in the last few months alone. In July 2025, the Trump administration announced its "AI Action Plan," in which maintaining a national security advantage in artificial intelligence is a primary concern.[16] As part of this initiative, the Department of Defense granted major American artificial intelligence companies like Anthropic and OpenAI a $200 million contract for access to their technology.[17] Models like Anthropic's Claude were soon thereafter cleared for handling classified information,[18] and their use quickly proliferated across the defense and intelligence communities.[19]

---

misuse of its then-existing authorities under the statute. KUERSTEN, *supra* note 8, at 10–11; 50 U.S.C. § 1881a(f)(2)(A).

11. *See* Justin Papp, *FISA Section 702: Congress Passes Short-Term Surveillance Program Extension Just Before Deadline*, CNBC (Apr. 30, 2026), https://www.cnbc.com/2026/04/30/fisa-section-702-congress-extension.html [https://perma.cc/D2AS-XQV5] (reporting that Congress passed a forty-five-day clean extension of Section 702 after the Senate rejected a three-year reauthorization, leaving the new statutory expiration date at June 12, 2026).

12. *But see* Meredith Lee Hill & Mia McCarthy, *GOP Leaders Delay FISA Vote amid GOP Rebellion*, POLITICO (Apr. 15, 2026), https://www.politico.com/news/2026/04/15/republicans-fisa-trump-house-00872766 [https://perma.cc/FV29-6PVC] (reporting on congressional gridlock despite presidential support).

13. *E.g.*, Government Surveillance Reform Act, S. 4082, 119th Cong. § 101 (2026); Mia McCarthy & Meredith Lee Hill, *Mike Johnson Faces FISA Mayhem*, POLITICO (Apr. 14, 2026), https://www.politico.com/live-updates/2026/04/14/congress/mike-johnson-faces-fisa-mayhem-00872465 [https://perma.cc/VS3J-HZBS].

14. *See* United States v. Hasbajrami, 945 F.3d 641, 645 (2d Cir. 2019) (dating the initial proceedings in one of the few judicial cases concerning Section 702 querying to 2011).

15. *See infra* subpart I(B).

16. MICHAEL J. KRATSIOS, DAVID O. SACKS & MARCO A. RUBIO, AMERICA'S AI ACTION PLAN 11, 16, 22 (2026), https://whitehouse.gov/wp-content/uploads/2025/07/Americas-AI-Action-Plan.pdf [https://perma.cc/5TXP-FNJA].

17. Justin Hendrix, *A Timeline of the Anthropic-Pentagon Dispute*, TECH POLICY PRESS (Mar. 19, 2026), https://www.techpolicy.press/a-timeline-of-the-anthropic-pentagon-dispute/ [https://perma.cc/W9Q5-7GYS].

18. *Id.*

19. *See, e.g.*, *How Spy Agencies Are Experimenting with the Newest AI Models*, THE ECONOMIST (July 29, 2025), https://www.economist.com/international/2025/07/29/how-spy-

Just a few months later, on January 3, 2026, the U.S. government conducted Operation Absolute Resolve, capturing Venezuelan President Nicolás Maduro,[20] and it soon became apparent that at least Anthropic's models were used in the operation.[21] Claude has since been reported as essential to U.S. targeting operations in Iran,[22] and companies like OpenAI have only strengthened their relationship with the U.S. government.[23] Even Anthropic, which recently fell out of favor with the Department of Defense, continues to support the use of its models for foreign intelligence purposes.[24]

Against this backdrop, this Note posits that understanding how artificial intelligence and Section 702 intersect in both their legal and technological capacities is essential. Part I maps the technical terrain that makes modern electronic surveillance possible. Part II describes the contours of Section 702 as the legal framework authorizing surveillance in environments shared by both unprotected foreign targets and protected U.S. persons. Part III reviews the case law analyzing Section 702's constitutionality with respect to the Fourth Amendment. Part IV then analyzes a novel change in Section 702 procedures and processes, likely centering around artificial intelligence-based technologies. This Note ultimately argues for human observability as the threshold factor in determining the validity of automated actions used in Section 702 surveillance.

I. The Internet and the Technology of Electronic Surveillance

This Part sketches how the United States uses the internet's physical architecture for foreign intelligence collection. It then offers a brief introduction to automation and large language models and explains how modern search engines can use these models. It concludes by placing these

agencies-are-experimenting-with-the-newest-ai-models [https://perma.cc/S68M-TQ4A] (reporting on the ever-increasing pressure for the Intelligence Community to adopt artificial intelligence tools in the face of mounting geopolitical competition).

20. Alexander Ward, Alex Leary, Dustin Volz, Vera Bergengruen & Shelby Holliday, *Inside Operation Absolute Resolve, the U.S. Incursion that Deposed Venezuela's Maduro*, WALL ST. J. (Jan. 3, 2026), https://www.wsj.com/politics/national-security/inside-operation-absolute-resolve-the-u-s-incursion-that-deposed-venezuelas-maduro-fa812617 [https://perma.cc/X49F-NXE7].

21. Amrith Ramkumar, Keach Hagey & Vera Bergengruen, *Pentagon Used Anthropic's Claude in Maduro Venezuela Raid*, WALL ST. J. (Feb. 15, 2026), https://www.wsj.com/politics/national-security/pentagon-used-anthropics-claude-in-maduro-venezuela-raid-583aff17 [https://perma.cc/AJ3X-2QTP]; Hendrix, *supra* note 17.

22. Hendrix, *supra* note 17.

23. Chris Vallance & Laura Cress, *OpenAI Changes Deal with U.S. Military after Backlash*, BBC (Mar. 3, 2026), https://www.bbc.com/news/articles/c3rz1nd0egro [https://perma.cc/Q4WX-LKYZ].

24. Dario Amodei, *Statement on Our Discussions with the Department of War*, ANTHROPIC (Feb. 26, 2026), https://www.anthropic.com/news/statement-department-of-war [https://perma.cc/BS4K-TBTR]; Sheera Frenkel, Cade Metz & Julian E. Barnes, *How Talks Between Anthropic and the Defense Department Fell Apart*, N.Y. TIMES (Mar. 1, 2026), https://www.nytimes.com/2026/03/01/technology/anthropic-defense-dept-openai-talks.html [https://perma.cc/EZ9L-BVV9].

machine-learning-enhanced search engines in the context of Section 702 and intelligence collection.

A. Networked Surveillance and the Internet

Spies, terrorists, and other provocateurs often rely on the internet—to conduct espionage, spread mayhem, or realize any number of other objectives. Everyone else also relies on the internet—to do their jobs, keep up with friends, or just run errands. All of this online activity, whether planning bomb plots or watching YouTube videos, is atomized into discrete packets upon transmission.[25] Later put back together, these packets contain content like portions of an email, along with header information like origin, destination, and error-correction data.[26] Specialized equipment dynamically routes data from computer to computer.[27] Depending on the moment, the most efficient path between neighboring computers can take a packet just around the block or all the way around the world.[28] These digital paths have physical underpinnings, with information flowing through an international web of cables spanning oceans and continents.[29]

The United States lies at the center of this web.[30] Warped by America's digital gravity, this international telecommunications network, or internet backbone, buttresses much of the United States' intelligence-gathering apparatus.[31] The United States' collection of internet-based target data is of two types: upstream and downstream.[32] Upstream collection uses the internet backbone to surveil data packets that are in transit between end users.[33] In contrast, downstream collection captures data stored by an electronic communication service provider like Google or Yahoo.[34] Taking advantage

25. PRIV. & C.L. OVERSIGHT BD., REPORT ON CERTAIN NSA USES OF XKEYSCORE FOR COUNTERTERRORISM PURPOSES 6 (2020) [hereinafter PCLOB XKEYSCORE REPORT].

26. ANDREW S. TANENBAUM & DAVID J. WETHERALL, COMPUTER NETWORKS 31, 33–34 (5th ed. 2011).

27. PCLOB XKEYSCORE REPORT, *supra* note 25, at 7.

28. *Id.* at 8.

29. *Id.* at 10–11. This web is also referred to as the "Internet backbone." PRIV. & C.L. OVERSIGHT BD., REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 60 (2023) [hereinafter PCLOB SECTION 702 REPORT].

30. Jack Goldsmith & Stuart Russell, *Strengths Become Vulnerabilities: How a Digital World Disadvantages the United States in Its International Relations* 2–3 (Hoover Working Grp. on Nat'l Sec., Tech. & L., Aegis Series Paper No. 1806, June 5, 2018), https://www.hoover.org/sites/default/files/research/docs/381100534-strengths-become-vulnerabilities.pdf [https://perma.cc/6GYU-2NNY].

31. *Id.*; *see* PCLOB SECTION 702 REPORT, *supra* note 29, at 167 (describing how access to the internet backbone enables collection from non-U.S. electronic communication service providers).

32. PCLOB SECTION 702 REPORT, *supra* note 29, at 59. Collection can also derive from a third, non-internet source: telephone communications. *Id.* at 64.

33. *Id.* at 60, 63.

34. *Id.* at 64.

of domestic technology companies' international market power, the United States government can compel American companies to provide information on targets located almost anywhere in the world.[35]

B. Googling for Foreign Intelligence: Information Retrieval and Electronic Surveillance

Intelligence agencies must store and search this collected surveillance data for it to be useful. But the databases searched and the querying software used by intelligence agencies are typically obfuscated by pages upon pages of redacted text.[36] This opacity around the technologies that underlie concerns about privacy intrusions and surveillance can be frustrating. However, these tools perform the same general functions as any other information-retrieval technology while operating at a scale similar to that of the internet itself.[37] A traditional internet search engine is thus analogous.[38] And a search engine enhanced with modern large language models likely approximates the classified processing actions and tools that intelligence agencies have recently adopted.[39]

1. A (Very) Brief Primer on Automation and Large Language Models.— Automation is a broad term, covering everything from ordinary thermostats to self-driving cars.[40] It also spans data science,[41] an interdisciplinary collection of

35. Goldsmith & Russell, *supra* note 30, at 3; 50 U.S.C. § 1881a(i)(1); PCLOB SECTION 702 REPORT, *supra* note 29, at 64.

36. *See, e.g.*, PCLOB XKEYSCORE REPORT, *supra* note 25, at 18–29 (redacting large swathes of information regarding an NSA querying technology).

37. *See* CHRISTOPHER D. MANNING, PRABHAKAR RAGHAVAN & HINRICH SCHÜTZE, INTRODUCTION TO INFORMATION RETRIEVAL 1 (2008) ("Information retrieval . . . is finding material (usually documents) of an unstructured nature (usually text) that satisfies an information need from within large collections (usually stored on computers)."); *cf.* Glenn Greenwald, *XKeyscore: NSA Tool Collects 'Nearly Everything a User Does on the Internet'*, GUARDIAN (July 31, 2013), https://www.theguardian.com/world/2013/jul/31/nsa-top-secret-program-online-data [https://perma.cc/E5DR-7J7R] (reporting on leaked information that describes the NSA's XKEYSCORE surveillance program as covering "nearly everything a typical user does on the internet" while at times ingesting amounts of information so large it "can only be stored for as little as 24 hours").

38. PCLOB SECTION 702 REPORT, *supra* note 29, at 88.

39. *See infra* subpart IV(A).

40. *See* Meg Leta Jones, *The Ironies of Automation Law: Tying Policy Knots with Fair Automation Practices Principles*, 18 VAND. J. ENT. & TECH. L. 77, 84 (2015) ("Broadly, automation includes all the ways computers and machines help people perform tasks more quickly, accurately, and efficiently.").

41. *See* ETHEM ALPAYDIN, INTRODUCTION TO MACHINE LEARNING 1–3 (2d ed. 2010) (explaining how computer algorithms store, process, and analyze large amounts of data); Jones, *supra* note 40, at 84 (stating that "data processing and decision making by computers" constitute a form of automation).

methods calculated to derive insights from data.[42] The models and tools arising out of this field exhibit a common tradeoff between interpretability and prediction quality.[43] The higher a model's predictive utility is, the harder it is to justify or explain that model's decisions *ex ante*.[44]

Machine learning tools are representative of this phenomenon. A type of artificial intelligence, machine learning models use specialized algorithms to learn patterns from provided datasets.[45] They can then apply these learnings to new fact patterns to make high-quality predictions.[46] Trained machine learning models are often described as "black boxes" impervious to human interpretation.[47] Such a characterization is exaggerated,[48] but it nonetheless reflects a common inability to explain any individual determination made by a machine learning model.[49] Despite this difficulty, contemporary automation efforts often rely on machine learning models to transform highly complicated real-world phenomena into computable systems with high predictive value, as recently demonstrated by large language models like those powering ChatGPT.[50]

Large language models are an especially versatile kind of machine learning model. These models have wide-ranging applications, including in database querying and information retrieval more generally.[51] Notably, large language models understand natural language and can impute semantic connections between different pieces of information rather than purely lexical or mathematical relationships.[52] Large language models can use this

42. Foster Provost & Tom Fawcett, *Data Science and Its Relationship to Big Data and Data-Driven Decision Making*, 1 BIG DATA 51, 52 (2013).

43. GARETH JAMES, DANIELA WITTEN, TREVOR HASTIE & ROBERT TIBSHIRANI, AN INTRODUCTION TO STATISTICAL LEARNING: WITH APPLICATIONS IN R 24–26 (2013).

44. *Id.* at 25–26.

45. Harry Surden, *ChatGPT, AI Large Language Models, and Law*, 92 FORDHAM L. REV. 1941, 1958 (2024).

46. *Id.*

47. *E.g.*, Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 886 (2016).

48. David Lehr & Paul Ohm, *Playing with the Data: What Legal Scholars Should Learn About Machine Learning*, 51 U.C. DAVIS L. REV. 653, 661 (2017).

49. Ashley S. Deeks, *Predicting Enemies*, 104 VA. L. REV. 1529, 1568 (2018).

50. Surden, *supra* note 45, at 1942–43.

51. Haoyi Xiong, Jiang Bian, Yuchen Li, Xuhong Li, Mengnan Du, Shuaiqiang Wang, Dawei Yin & Sumi Helal, *When Search Engine Services Meet Large Language Models: Visions and Challenges*, ARXIV, at 1–2 (June 28, 2024), https://arxiv.org/pdf/2407.00128v1 [https://perma.cc/CRA2-Q9GW].

52. Surden, *supra* note 45, at 1947, 1964–65. In contrast, a typical lexical search will compare the keywords contained in a query with keywords contained in any searched documents and will go no further. *Cf.* Saar Kuzi, Mingyang Zhang, Cheng Li, Michael Bendersky & Marc Najork, *Leveraging Semantic and Lexical Matching to Improve the Recall of Document Retrieval Systems: A Hybrid Approach*, ARXIV (Oct. 2, 2020), https://arxiv.org/pdf/2010.01195v1 [https://perma.cc/M8NV-CCS4] (describing this lexical search function in search engines).

ability to extract information from documents external to the datasets with which they were trained.[53] They can even compare different external documents without directly relying on their training data for insights.[54]

2. Search Engines as a Proxy for Section 702 Querying.—A large-language-model-enabled search engine likely approximates the redacted automated processes and tools that were recently approved for use by the NSA and CIA.[55] These enhanced search engines build upon traditional search-engine technology and incorporate novel large language models to extract deeper meaning from searched data.

The traditional search engine relies on four key operations: (1) crawling, (2) indexing, (3) retrieval,[56] and (4) ranking.[57] First, *crawling* involves a constant process of mapping the internet and documenting as many websites as possible.[58] Second, these website documents are built into an *index*, i.e., a database of crawled documents.[59] The traditional search-engine index is known as an inverted index,[60] less commonly but more usefully called a lexical index.[61] The lexical index consists of two components: a lexicon and postings lists.[62] The lexicon is a list of terms, and each term has a corresponding postings list that tracks every document in which the term appears.[63] Modern search engines' indices are massive affairs that span billions of documents.[64] Third, because a direct query of the full index could return millions of results, search engines utilize a *retrieval* system to reduce the number of results to the thousands.[65] Typically, retrieval systems associate relevance scores to documents that share terms with a query.[66] They then use this score to retrieve a pared down list of documents.[67] Fourth, the

53. Meor Amer & Maxime Voisin, *From RAG to Tool Use*, COHERE, https://cohere.com/llmu/from-rag-to-tool-use [https://perma.cc/7ERA-Y96Z].

54. *Id.*

55. *See infra* subpart IV(A).

56. Note that the term "retrieval" in the search-engine context is distinct from the term "retrieval" in the Section 702 context.

57. United States v. Google LLC, 747 F. Supp. 3d 1, 38–39 (D.D.C. 2024).

58. *Id.* at 38; Xiong et al., *supra* note 51, at 2–3.

59. *Google*, 747 F. Supp. at 38.

60. Xiong et al., *supra* note 51, at 3.

61. *See, e.g.*, Kuzi et al., *supra* note 52 (referring to an inverted index as a lexical index).

62. MANNING ET AL., *supra* note 37, at 6.

63. *Id.*

64. *See Google*, 747 F. Supp. at 39 (describing an internal company index at Apple encompassing billions of websites).

65. *Id.*

66. Kuzi et al., *supra* note 52.

67. *Id.*; *see also* MANNING ET AL., *supra* note 37, at 136–37.

retrieved list is then *ranked* for relevance using various algorithms.[68] The final results of this ranking are provided to the end user.[69]

Modern search engines supplement every stage of the traditional search process with machine learning models.[70] Large language models in particular have been especially transformative.[71] From some underlying text or document, large language models can extract numerical "word vectors" or "word embeddings," which encode for meaning, and then mathematically compare them to ascertain their semantic similarity.[72] Accordingly, search engines empowered with large language models can interpret both documents' and queries' underlying conceptual meanings.[73] This semantic understanding helps generate richer search results that are more faithful to the meaning underlying both inputted queries and outputted documents.[74]

This semantic search mirrors the traditional lexical search framework.[75] After the crawling stage, the semantic search engine's large language model will interpret crawled documents and create vectors or embeddings for each.[76] These document embeddings together form a semantic index.[77] When presented with a query, the semantic search engine will similarly generate an embedding from the query.[78] At the retrieval stage, the semantic search engine compares this query embedding against the semantic index to pull sufficiently similar documents.[79] For the final ranking stage, these semantic retrieval results will be sorted—and likely mixed with retrieval results from a traditional lexical search running in parallel—before being served to the end user.[80]

---

68. *Google*, 747 F. Supp. at 39. The most famous of these ranking algorithms is Google's PageRank. *See* Sergey Brin & Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, 30 COMPUT. NETWORKS & ISDN SYS. 107, 109 (1998) (describing PageRank as "an excellent way to prioritize the results of Web keyword searches").

69. *Google*, 747 F. Supp. at 39.

70. *Id.* at 53; Xiong et al., *supra* note 51, at 1.

71. *Google*, 747 F. Supp. at 53.

72. Surden, *supra* note 45, at 1965–66.

73. Xiong et al., *supra* note 51, at 8–9.

74. *See, e.g.*, Kuzi et al., *supra* note 52, at tbl.1 (illustrating how a model with semantic understanding can retrieve more relevant and useful documents than a purely lexical model).

75. Because of its likely similarity with the CIA processing tool discussed *infra* section IV(A)(2), this description of a semantic search engine relies heavily on the proposed hybrid lexical-semantic search engine described in Kuzi et al., *supra* note 52. For a useful graphical depiction of this proposed search engine, see *id.* at fig.1.

76. *Id.*

77. *Id.*

78. *Id.*

79. *See id.* (explaining how semantic similarities between queries and documents are measured).

80. *Id.*

The large-language-model-enabled search engine thus described is likely analogous to the automated CIA processing tool and NSA processing procedures discussed below. The CIA processing tool serves as a representative example. Based on the available unredacted information, the CIA tool processes data upon collection,[81] similar to how the described semantic search engine creates its semantic index from crawled documents. If queried after this indexing stage, the CIA tool also likely performs similar retrieval and ranking functions as the described model. Both models automatically process ingested data, but neither model acts any further unless prompted with a query.[82] Public and leaked Intelligence Community documents and recent reporting further bolster the search-engine analogy. Redacted government reports and leaked NSA documents both demonstrate search-engine-like capabilities,[83] and American intelligence agencies are reportedly making large investments to quickly deploy large-language-model systems.[84]

II. An Overview of Section 702

The legal application of the technological architecture discussed above hinges on a critical distinction between what is domestic and what is foreign.[85] This difference underpins the legal authorities that enable and empower the American Intelligence Community.[86] The Intelligence Community today draws its affirmative authority for electronic surveillance from three general sources: (1) Executive Order 12333, as supplemented by Executive Order 14086;[87] (2) Title I of the Foreign Intelligence Surveillance

81. *In re* DNI/AG 702(h) Certification 2024-A & Its Predecessor Certifications, No. 702(j)-24-01, slip op. at 33 (F.I.S.C. Apr. 4, 2024) [hereinafter 2024 FISC Opinion].

82. *See infra* section IV(A)(2).

83. *See* PCLOB XKEYSCORE REPORT, *supra* note 25, at 20, 24 (using similar terminology as that used to describe search engines, with a focus on indexing as a key component of a surveillance search system); Greenwald, *supra* note 37 (sharing leaked NSA training slides that demonstrate search-engine-like capabilities).

84. *How Spy Agencies Are Experimenting with the Newest AI Models*, *supra* note 19.

85. Adam Klein, *National Security Surveillance in the United States: Laws, Institutions, and Safeguards*, STRAUSS CTR. FOR INT'L SEC. & L. 15 (Nov. 15, 2023), https://safeandfree.io/wp-content/uploads/USA_Surveillance_Final.pdf [https://perma.cc/H922-B7NA]; *see also* Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 HARV. J.L. & PUB. POL'Y 117, 147–48 (2015) (explaining how Congress "explicitly exempted foreign-to-foreign wire communications from FISA's remit," thereby "grounding the exception in territorial limits").

86. The Intelligence Community, as established by statute or executive order, encompasses eighteen organizations, including, but not limited to, the CIA, the NSA, and parts of the FBI. OFF. OF THE DIR. OF NAT'L INTEL., MEMBERS OF THE IC, https://www.dni.gov/index.php/what-we-do/members-of-the-ic [https://perma.cc/ET5E-UUZK].

87. Exec. Order No. 12,333, 3 C.F.R. § 200 (1981), *reprinted as amended in* 50 U.S.C. § 3001 app. at 148–57 (2018) [hereinafter Exec. Order No. 12,333]; Exec. Order No. 14,086, 87 Fed. Reg. 62283 (Oct. 7, 2022) [hereinafter Exec. Order No. 14,086].

Act,[88] or traditional FISA;[89] and (3) Section 702 of the FISA Amendments Act.[90]

These authorities divide responsibilities and assign obligations based on the status of a target (whether a U.S. person or not),[91] the location of a target (whether inside the United States or outside),[92] and the point of collection for the target's information (whether within the United States or without).[93] Traditional overseas collection—surveillance that occurs outside the United States against a non-U.S. person located abroad—falls under the purview of Executive Orders 12333 and 14086.[94] Electronic surveillance that is collected within the United States and targets anyone—regardless of their U.S.-person status—located in the United States, however, must also comply with traditional FISA.[95] Section 702 governs in the hybrid scenario where a non-U.S. person target is located abroad but the surveillance is still collected within the United States.[96]

A. Executive Order 12333 and Traditional FISA

Executive Order 12333 and traditional FISA form opposite ends of a spectrum, with Section 702 in between. Executive Order 12333 allows for warrantless electronic surveillance, whereas traditional FISA requires a warrant. Though distinct fact patterns trigger each authority, the advent of the internet weakened these distinctions. Section 702 responds to this tension.

Executive Order 12333 provides the general organizing principle for the Intelligence Community and sets the baseline for its foreign intelligence

88. 50 U.S.C. §§ 1801–13.

89. The phrase "traditional FISA" also covers Title III, which extends Title I's electronic-surveillance regime to physical searches but is not relevant to this discussion. 50 U.S.C. §§ 1821–29.

90. 50 U.S.C. § 1881a.

91. A U.S. person is either a citizen, a lawful permanent resident, an unincorporated association with a substantial number of members who are U.S. citizens or lawful permanent residents, or a corporation incorporated in the United States but not controlled by a foreign power. Exec. Order No. 12,333, *supra* note 87, § 3.5(k); Exec. Order No. 14,086, *supra* note 87, § 4(i), (m); 50 U.S.C. § 1801(i).

92. In this context, "inside the United States" means being physically located within the geographic territory of the United States. 50 U.S.C. §§ 1801(j), 1881a(b).

93. In contrast, "within the United States" here means using U.S.-based internet or telecommunications infrastructure to collect communications. 50 U.S.C. § 1881a(i)(1).

94. Donohue, *supra* note 85, at 144–45; Matthew Connolly, *Will the EU-US Data Privacy Framework Survive* Schrems III*?*, 27 TRINITY COLL. L. REV. 87, 106–08 (2024).

95. *See* 50 U.S.C. § 1801(f) (defining "[e]lectronic surveillance" under FISA to include the acquisition of any communications to or from a person in the U.S.); *cf.* Donohue, *supra* note 85, at 146 (affirming that all electronic surveillance must comport with both FISA and Executive Order 12333).

96. 50 U.S.C. § 1881a(a)–(b).

activities.[97] The order grants the NSA exclusive authority to collect signals intelligence.[98] In addition to authorizing the canonical extraterritorial surveillance of non-U.S. persons located abroad, Executive Order 12333 also contemplates the Intelligence Community surveilling U.S. persons.[99] Any efforts targeting U.S. persons must comply with Attorney General-approved guidelines[100] and must constitute the least intrusive means of collection possible.[101] But least intrusive does not mean unintrusive. Techniques targeting U.S. persons that would require a warrant in the law enforcement context are available but subject to higher scrutiny.[102] Such techniques must still comply with relevant statutory regimes like FISA, and they depend on the Attorney General's case-by-case determination that there is probable cause to think the target is or is an agent of a foreign power.[103] Executive Order 14086 supplements Executive Order 12333, extending many of these U.S.-person procedural safeguards to non-U.S. persons from qualifying countries.[104]

Traditional FISA is the exclusive statutory authority for electronic surveillance conducted against U.S. or non-U.S. persons located in the United States for foreign intelligence purposes.[105] As such, traditional FISA subsumes Executive Order 12333 to the extent the two overlap.[106] Under FISA, the government must obtain an order from a specialized court to conduct surveillance targeting a U.S. person or occurring in the United

97. PRIV. & C.L. OVERSIGHT BD., EXECUTIVE ORDER 12333, 4 (2021) [hereinafter PCLOB EXEC. ORDER 12333 REPORT]. Executive Order 12333 also delineates each element of the Intelligence Community's affirmative responsibilities, reserving, for example, covert action activities to the CIA. Exec. Order No. 12,333, *supra* note 87, § 1.7(a)(4).

98. Exec. Order No. 12,333, *supra* note 87, § 1.7(c)(2). There are some exceptions for the FBI. PCLOB EXEC. ORDER 12333 REPORT, *supra* note 97, at 16.

99. Exec. Order No. 12,333, *supra* note 87, § 2.3.

100. *E.g.*, NAT'L SEC. AGENCY, U.S. SIGNALS INTEL. DIRECTIVE SP0018, LEGAL COMPLIANCE AND U.S. PERSONS MINIMIZATION PROCEDURES (2011), https://www.eff.org/files/2013/11/21/20131119-odni-united_states_signals_intelligence_directive_18_jan_25_2011.pdf [https://perma.cc/9GRD-MAFY].

101. Exec. Order No. 12,333, *supra* note 87, § 2.4. The order also expressly limits the kinds of information that the Intelligence Community can seek to ten categories. *Id.* § 2.3.

102. *Id.* § 2.5.

103. *Id.*

104. Exec. Order No. 14,086, *supra* note 87, §§ 1, 3(f).

105. 50 U.S.C. §§ 1801(f), 1812(a); Mark M. Jaycox, *No Oversight, No Limits, No Worries: A Primer on Presidential Spying and Executive Order 12,333*, 12 HARV. NAT'L SEC. J. 58, 71–72 (2021). Electronic surveillance here includes wiretapping, radio surveillance, and physical bugs. 50 U.S.C. § 1801(f).

106. PCLOB EXEC. ORDER 12333 REPORT, *supra* note 97, at 14; *see* Jaycox, *supra* note 105, at 75 (explaining that Executive Order 12333 only governs surveillance activities that do not fall under FISA).

States.[107] This court, the Foreign Intelligence Surveillance Court (FISC),[108] will grant the order upon a showing of probable cause that the proposed target is or is an agent of a foreign power.[109] The FISC order is essentially equivalent to a traditional warrant.[110] Without this requirement, targeting deliberations would occur wholly within the Executive Branch. Instead, FISC orders require the government to submit specific, reasoned applications to an independent tribunal.[111]

By the turn of the twenty-first century, these order requirements proved a significant constraint on surveillance efforts for foreign intelligence.[112] The United States presided over a global internet where non-U.S. persons—including bona fide targets like terrorists and spies—communicated and planned using American infrastructure. And they could do so without ever setting foot inside the United States. In this new environment, collection efforts previously regulated by Executive Order 12333 increasingly fell under the purview of traditional FISA.[113] The interplay between the two resulted in targets with no U.S. nexus receiving inordinate legal protection.[114] As the government strained these authorities to fit the new intelligence environment, Congress eventually enacted Section 702 to remedy this tension.[115]

---

107. *See* 50 U.S.C. § 1803(a)–(b) (establishing a specialized court comprised of district court judges to "hear applications for and grant orders approving electronic surveillance anywhere within the United States[,]" as well as a specialized court of review).

108. *Id.* § 1803(a). Congress also created the Foreign Intelligence Surveillance Court of Review (FISCR) with appellate jurisdiction over the FISC. *Id.* § 1803(b). Both of these courts are clothed in the garb of Article III, but they push at the limits of the mainstream view of Article III courts' overarching purpose and jurisdiction. *See, e.g.*, United States v. Muhtorov, 20 F.4th 558, 681–83 (10th Cir. 2021) (Lucero, J., dissenting) (arguing that the FISC's determinations are advisory opinions in violation of Article III).

109. 50 U.S.C. § 1805(a)(2)(A).

110. *See* United States v. Cavanagh, 807 F.2d 787, 790–91 (9th Cir. 1987) (holding that the FISC serves as a neutral and detached body and that FISA's requirements satisfy Fourth Amendment probable cause and particularity requirements); Donohue, *supra* note 85, at 204 ("FISA . . . is the *de facto* Fourth Amendment standard for the contours of the warrant clause for electronic intercepts on U.S. soil.").

111. 50 U.S.C. § 1804(a).

112. *See* Donohue, *supra* note 85, at 146–47 (writing that in 2006, the Director of National Intelligence argued that because surveillance efforts increasingly fell under FISA's stricter requirements, the intelligence community was only collecting one-third of the foreign intelligence information it had previously collected).

113. *Id.* at 146.

114. Brittany Adams, Comment, *Striking a Balance: Privacy and National Security in Section 702 U.S. Person Queries*, 94 WASH. L. REV. 401, 410 (2019); Donohue, *supra* note 85, at 147–48.

115. *See* Adams, *supra* note 114, at 406–09 (describing how Congress enacted Section 702 in response to concerns about the overly prohibitive and burdensome requirements under FISA); United States v. Muhtorov, 20 F.4th 558, 586 (10th Cir. 2021) (explaining that Section 702 was passed to help the intelligence community "meet the challenges of modern technology and international terrorism" (quoting *Clapper v. Amnesty Int'l*, 568 U.S. 398, 403–04 (2013))).

B. Section 702: A Procedural Scheme

Section 702 is a functional hybrid between Executive Order 12333 and traditional FISA.[116] Like under Executive Order 12333, the government maintains significant discretion in selecting non-U.S. person targets for electronic surveillance.[117] And like under traditional FISA, Section 702 still involves some judicial scrutiny.[118] However, this scrutiny is materially different.[119] Under Section 702, the FISC does not approve surveillance orders on a case-by-case basis.[120] Instead, it approves the procedures by which the government selects its targets and controls and searches the information collected.[121] The FISC reviews whether these procedures comport with both the Fourth Amendment and the statutory requirements of Section 702.[122] Accordingly, Section 702 surveillance's legal validity is centered on its procedures.[123]

Section 702 surveillance takes the following basic form. Only four agencies—NSA, CIA, FBI, and National Counterterrorism Center—have access to Section 702 collection data.[124] The statute only allows targeting non-U.S. persons reasonably believed to be located outside the United States for foreign intelligence purposes.[125] The government has two avenues for surveilling these targets—upstream and downstream collection.[126] The NSA undertakes all upstream collection[127] and receives the resulting unminimized,

116. For a more comprehensive discussion of how Section 702 works, see generally PCLOB SECTION 702 REPORT, *supra* note 29.

117. *Cf.* Donohue, *supra* note 85, at 147–48 (explaining that one of the strongest arguments for enacting Section 702 was to restore the laxer pre-internet protections afforded to foreign-to-foreign communications conducted by non-U.S. persons).

118. *E.g.*, 50 U.S.C. § 1881a(d)(2).

119. *See* Adams, *supra* note 114, at 409–10 (noting how Section 702 weakens traditional FISA's protections).

120. *See* 50 U.S.C. § 1881a(c) (requiring decisions to target to be made in accordance with generalized targeting procedures rather than a case-specific FISC order).

121. *See id.* § 1881a(d)(2), (e)(2), (f)(1)(C) (providing for judicial review of Section 702 targeting, minimization, and querying procedures).

122. 2024 FISC Opinion, *supra* note 81, at 9 (citing 50 U.S.C. § 1881(j)(1)(A), (j)(2)).

123. *Id.* Where U.S.-person information is not present, different authorities and procedures govern, namely Executive Orders 12333 and 14086. PCLOB SECTION 702 REPORT, *supra* note 29, at 82 n.126.

124. PCLOB SECTION 702 REPORT, *supra* note 29, at 5–6.

125. 50 U.S.C. § 1881a(a). The nominating and targeting agencies must make both a foreignness determination and an affirmative foreign intelligence-purpose determination. PCLOB SECTION 702 REPORT, *supra* note 29, at 67–68.

126. PCLOB SECTION 702 REPORT, *supra* note 29, at 59.

127. The NSA, by virtue of Section 702, will compel U.S. companies operating portions of the internet backbone to provide traffic to or from the selected targets. 50 U.S.C. § 1881a(i)(1); PCLOB SECTION 702 REPORT, *supra* note 29, at 60. Though traffic between non-targets containing content about the target can and has been collected previously, the NSA does not currently practice this "abouts" collection. PCLOB SECTION 702 REPORT, *supra* note 29, at 61. Companies compelled may dispute collection orders but have limited avenues to do so. 50 U.S.C. § 1881a(i)(4).

or raw, data.[128] It forwards this data to other agencies only after applying its own minimization procedures.[129] The FBI cosigns all downstream collection[130] and receives the resulting unminimized raw data.[131] The FBI sends this data to other agencies in its unminimized form.[132]

To carry out this surveillance process, the relevant agencies use three types of procedures: (1) targeting procedures, (2) minimization procedures, and (3) querying procedures.

1. Targeting Procedures.—As only the NSA and FBI are involved with the actual collection process, they are the only agencies with FISC-approved targeting procedures.[133] The NSA's targeting procedures require it to first determine, based on the totality of the circumstances, that any potential target is a non-U.S. person located outside the United States.[134] In making this determination, an NSA analyst will look to at least one of the following: (1) the information that prompted their interest in the target in the first place, (2) information the NSA already knows or can infer about where the target is located, and (3) classified NSA tools that can further help confirm the target's location.[135] If the potential target is reasonably thought to be abroad, the analyst will also look to his U.S.-person status.[136] In the event she cannot confirm his status, the NSA analyst will presume the potential target is a non-U.S. person.[137] The analyst must also make her own particularized, fact-based judgment that the potential target is a reasonable source of foreign intelligence.[138] If she determines the potential target is such a source, the NSA analyst can proceed to actually target him.[139] Post-targeting, the NSA will re-confirm the target's

128. PCLOB SECTION 702 REPORT, *supra* note 29, at 61.

129. *Id.*

130. The FBI, by virtue of Section 702, will compel U.S. providers operating internet services like email or file storage to provide the selected target's traffic. 50 U.S.C. § 1881a(i)(1); PCLOB SECTION 702 REPORT, *supra* note 29, at 64. Compelled companies may dispute this collection order but have limited avenues to do so. 50 U.S.C. § 1881a(i)(4).

131. PCLOB SECTION 702 REPORT, *supra* note 29, at 64–65.

132. *Id.* at 65. The NSA also receives a copy of all downstream collection, regardless of the nominating agency. *Id.*

133. *Id.* at 66. The other agencies will nominate targets and provide the relevant information to the NSA or FBI as required. *Id.* Each of these two agencies must then apply its own targeting procedures before proceeding to collect on the nominated target. *Id.*

134. NAT'L SEC. AGENCY, PROCEDURES FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES 1–2 (2023), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2024/2024_Cert_NSA_TPs_for_Public_Redacted_3-13-23.pdf [https://perma.cc/JL6Q-A397].

135. *Id.*

136. *Id.* at 4.

137. *Id.*

138. *Id.*

139. The analyst at this point has exhausted all hurdles to initiating targeting. *See id.* at 1–6 (lacking further pre-targeting procedures).

location and U.S.-person status.[140] If the NSA determines that the target was in fact in the United States or was a U.S. person, it will stop any further targeting and document the occurrence.[141] The NSA's targeting procedures further describe rules and processes regarding documentation, oversight, and emergency exceptions.[142]

The FBI's targeting procedures mandate that it receive an explanation from the NSA regarding its determination of the proposed target's location and U.S.-person status.[143] The FBI must then corroborate this determination before going forward with collection.[144] If either the NSA or FBI later discover the target is ineligible for targeting, the discovering agency will notify the other.[145] The FBI will stop further collection until it can reestablish the target's eligibility.[146] As with the NSA's targeting procedures, the FBI's procedures also provide additional details regarding documentation, oversight, and emergency exceptions.[147]

2. Minimization and Querying Procedures.—All agencies must also have their own FISC-approved minimization and querying procedures.[148] Though each agency's minimization procedures are tailored to its particular intelligence mission, they all share similar characteristics.[149] These procedures seek to "minimize" the use of otherwise unavailable U.S.-person information.[150] To this end, agencies will delete irrelevant U.S.-person information.[151] And unless necessary for understanding the attached foreign intelligence or depicting evidence of a crime, all agencies generally mask identifiable U.S.-person information with generic terms before its use or dissemination to other agencies.[152] Minimization also includes a host of other, less obvious

140. *Id.* at 6–7.

141. *Id.* at 6–7, 10.

142. *Id.* at 9–11.

143. FED. BUREAU OF INVESTIGATION, PROCEDURES FOR TARGETING NON-UNITED STATES PERSONS REASONABLY BELIEVED TO BE LOCATED OUTSIDE THE UNITED STATES 2 (2023), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2024/2024_Cert_FBI_TPs_for_Public_Redacted_3-13-23.pdf [https://perma.cc/79ZC-HCZJ].

144. *Id.*

145. *Id.* at 6–7.

146. *Id.* at 7.

147. *Id.* at 5–7.

148. 50 U.S.C. § 1881a(e)(1)–(2), (f)(1)(A)–(C), (j)(2)(C)–(D).

149. PCLOB SECTION 702 REPORT, *supra* note 29, at 74.

150. 50 U.S.C. § 1801(h)(1).

151. *E.g.*, NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION 5 (2023), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2024/2024_Cert_NSA_MPs__for_Public_Redacted_3-13-23.pdf [https://perma.cc/9EJW-XP26] [hereinafter 2023 NSA MINIMIZATION PROCEDURES].

152. *E.g.*, *id.* at 14–15.

requirements that serve to decrease the probability of improperly using U.S.-person information. These include training requirements, data retention and purging rules, and special treatment for privileged communications like attorney–client privilege.[153]

Each agency also has FISC-approved querying procedures for searching through unminimized Section 702 data. A query[154] is akin to an internet search through existing stores of already collected but unminimized Section 702 information.[155] Each agency's querying procedures generally follow a similar three-prong standard.[156] Before an analyst queries a Section 702 database, she must first (1) have a foreign-intelligence purpose,[157] (2) use terms that are not overly broad, and (3) have a recorded, fact-based justification.[158] For the NSA and FBI, additional constraints supplement this general standard.[159] However, both agencies have had issues

153. *E.g.*, *id.* at 1, 9, 10, 13.

154. Query is statutorily defined as "the use of one or more terms to retrieve the unminimized contents or noncontents located in electronic and data storage systems of communications of or concerning United States persons obtained through [Section 702] acquisitions." 50 U.S.C. § 1881a(f)(5)(B). Simplifying this language, querying is, at its core, akin to searching for a term in a text document using the Ctrl-F function present in most word processors. *Cf.* Orin S. Kerr, *Data Scanning and the Fourth Amendment*, 67 BOS. COLL. L. REV. 431, 436–39 (2026) (explaining the basics of electronic data searches).

155. PCLOB SECTION 702 REPORT, *supra* note 29, at 88.

156. *Id.* at 92–93. But exceptions exist. *E.g.*, NAT'L SEC. AGENCY, QUERYING PROCEDURES USED IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION 5–6 (2023), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2024/2024_Cert_NSA_QPs_for_Public_Redacted_3-13-23.pdf [https://perma.cc/LPC9-35YK] [hereinafter 2023 NSA QUERYING PROCEDURES].

157. The NSA also conducts travel-vetting queries that are not governed by the general querying procedures mandated by Section 702; as such, this Note does not discuss them in detail. 2023 NSA QUERYING PROCEDURES, *supra* note 156, at 6–7; *In re* DNI/AG 702(h) Certification 2023-A & Its Predecessor Certifications, No. 702(j)-23-01, slip op. at 44, 56–59 (F.I.S.C. Apr. 11, 2023) [hereinafter 2023 FISC Opinion].

158. 2023 NSA QUERYING PROCEDURES, *supra* note 156, at 1, 4–5; CENT. INTEL. AGENCY, QUERYING PROCEDURES USED IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION 1, 3–4 (2019), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2024/2024_Cert_CIA_QPs_for_Public_Redacted_3-13-23.pdf [https://perma.cc/SJ78-CZC9] [hereinafter 2019 CIA QUERYING PROCEDURES]; FED. BUREAU OF INVESTIGATION, QUERYING PROCEDURES USED IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION 1, 3–5 (2024), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2024/2024_Cert_FBI_QPs_for_Public_Redacted_3-13-23.pdf [https://perma.cc/9T7R-NPDZ]; NAT'L COUNTERTERRORISM CTR., QUERYING PROCEDURES USED IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION 1, 3–4 (2020), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/2024/2024_Cert_NCTC_QPs_for_Public_Redacted_3-13-23.pdf [https://perma.cc/FUD7-3TYW]; PCLOB SECTION 702 REPORT, *supra* note 29, at 93–94.

159. For example, NSA analysts must obtain prior approval from the NSA's Office of General Counsel before querying with a U.S.-person term. 2023 NSA QUERYING PROCEDURES, *supra* note 156, at 4. In contrast, the CIA and National Counterterrorism Center "maintain [neither] unique [nor] nuanced query authority." PCLOB SECTION 702 REPORT, *supra* note 29, at 105.

complying with their querying procedures in the past.[160] The FBI has an especially egregious track record,[161] though internal structural changes,[162] recent FBI-focused amendments to Section 702,[163] and updated FISC-approved procedures[164] might lead to fewer issues in the future.

III. Section 702 Surveillance and the Fourth Amendment

The impetus behind Section 702's procedures is to protect U.S. persons from unreasonable invasions of privacy without affording non-U.S. persons those same protections.[165] The Fourth Amendment is the ordinary protector of this expectation of privacy, but non-U.S. persons normally have no such protection.[166] Section 702 tries to statutorily thread the needle through situations where U.S. persons' data, which implicates individuals' constitutionally protected privacy interests, are mixed with non-U.S. persons' foreign activity, which implicates the government's legitimate national security interests.[167] In lawfully targeting non-U.S. persons, the government may incidentally collect the communications of U.S. persons.[168] Under the Fourth Amendment, the reasonableness of the collection itself is fairly uncontroversial.[169] However, the reasonableness of any post-collection querying of U.S.-person information is not.[170] Crucially, the limitations

160. PCLOB SECTION 702 REPORT, *supra* note 29, at 104–05.

161. *Id.* at 142.

162. *See, e.g.*, *id.* at 111 (noting a recent reform requiring pre-query approval by an attorney for all batch queries conducted by the FBI).

163. *See* Reforming Intelligence and Securing America Act, Pub. L. No. 118-49, § 3, 138 Stat. 862, 866–67 (2024) (codified as amended at 50 U.S.C. § 1881a(f)(2)(A)–(B)) (amending Section 702 to, among other things, prohibit the FBI from conducting queries for the sole purpose of finding evidence of a crime with limited exceptions).

164. *See* 2024 FISC Opinion, *supra* note 81, at 2, 24 (approving the 2024 FBI querying procedures and noting new modifications that are likely to improve compliance).

165. *See* 50 U.S.C. § 1881a(b) (prohibiting acquisitions targeting U.S. persons or persons located in the U.S. and requiring compliance with the Fourth Amendment); 2023 FISC Opinion, *supra* note 157, at 38–39 (interpreting Section 702 requirements as "aimed at guarding against unreasonable intrusions into U.S.-person communications").

166. *See* Katz v. United States, 389 U.S. 347, 360–61 (1967) (Harlan, J. concurring) (articulating the "reasonable expectation of privacy" test that defines the Fourth Amendment's protection of individual privacy); United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990) (holding that the Fourth Amendment does not apply to searches conducted outside the United States against non-U.S. citizens or residents).

167. Adams, *supra* note 114, at 409–11.

168. PCLOB SECTION 702 REPORT, *supra* note 29, at 97.

169. *See* 2024 FISC Opinion, *supra* note 81, at 26 (noting that all Courts of Appeals that have considered the issue have found incidental collection of U.S.-person information reasonable).

170. *Contrast id.* at 29–31 (finding post-collection querying constitutionally reasonable in light of the constraints placed by targeting, minimization, and querying procedures), *and* United States v. Mohamud, 843 F.3d 420, 443 (9th Cir. 2016) (affirming the district court's finding that post-collection querying was constitutionally reasonable in light of the targeting and minimization procedures that existed at the time), *with* United States v. Hasbajrami, 945 F.3d 641, 672 (2d Cir.

imposed by Section 702's targeting, minimization, and querying rules play an essential role in establishing the constitutionality of both Section 702 generally and post-collection querying specifically.[171]

A. Incidental Collection and the Fourth Amendment

The FISCR[172] and the Second, Ninth, and Tenth Circuit Courts of Appeals have found incidental collection of U.S.-person information to be reasonable under the Fourth Amendment.[173] The Fourth Amendment protects the "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches . . . ."[174] As such, the Fourth Amendment typically requires the government to obtain a warrant based on probable cause before conducting a search.[175] But a foreign-intelligence exception to this warrant requirement exists, and the Fourth Amendment's protections do not extend to non-U.S. persons located abroad.[176] All four courts saw collection under Section 702 surveillance programs as permissible under these paradigms.[177]

However, the inquiry does not stop there. Even when no warrant is required, the Fourth Amendment still requires government searches to be reasonable.[178] In determining reasonableness, courts apply a totality-of-the-circumstances balancing test, weighing the severity of the governmental intrusion into individual privacy rights against the necessity of the intrusion to the government's interests.[179] Only the four aforementioned appellate courts have reviewed the reasonableness of Section 702's collection of incidental U.S.-person information, with each finding the incidental collection reasonable.

2019) (considering post-collection querying as likely unconstitutional unless a Fourth Amendment reasonableness inquiry is made with each individual query), *and* United States v. Muhtorov, 20 F.4th 558, 604 (10th Cir. 2021) (stating that post-collection querying to collect evidence for trial could raise Fourth Amendment concerns).

171. *E.g.*, 2024 FISC Opinion, *supra* note 81, at 26, 29, 32.

172. *See supra* note 108.

173. *Muhtorov*, 20 F.4th at 593; *Hasbajrami*, 945 F.3d at 662; United States v. Mohamud, 843 F.3d 420, 439 (9th Cir. 2016); *see In re* Directives Pursuant to Section 105B of FISA, 551 F.3d 1004, 1015 (F.I.S.C.R. 2008) (finding incidental collection lawful under a predecessor statute to Section 702).

174. U.S. CONST. amend. IV.

175. Riley v. California, 573 U.S. 373, 382 (2014) (citing Vernonia Sch. Dist. 47J v. Acton, 515 U.S. 646, 653 (1995)).

176. *In re Directives*, 551 F.3d at 1011–12; United States v. Verdugo-Urquidez, 494 U.S. 259, 274–75 (1990).

177. *In re Directives*, 551 F.3d at 1012; *Muhtorov*, 20 F.4th at 593; *Hasbajrami*, 945 F.3d at 662; *Mohamud*, 843 F.3d at 439.

178. Maryland v. King, 569 U.S. 435, 448 (2013).

179. *Id.*

All four courts found the governmental interest in foreign intelligence to be largely decisive.[180] Other arguments favoring reasonableness included appeals to the third-party, incidental-overhear, and plain-view doctrines. In *United States v. Mohamud*, the Ninth Circuit viewed the targeted non-U.S. person as a third party with whom the defendant had shared information, thereby weakening his reasonable expectation of privacy in that information.[181] In *United States v. Hasbajrami*, the Second Circuit drew a similarity between incidentally acquired U.S.-person information and incidentally overheard criminal conversations, which have reduced expectations of privacy.[182] In *United States v. Muhtorov*, the Tenth Circuit elaborated on this reasoning as it relates to the plain-view doctrine.[183] The court concluded that incidentally collected U.S.-person information satisfies the three elements of the plain-view doctrine.[184] The court found that (1) the root search was lawfully directed at a non-U.S. person and (2) the two-way nature of communications necessarily meant that the government has lawful access to incidental communications with the target.[185] The facts of the case made the third element, that the seized information be clearly incriminating, a non-issue.[186] Section 702's FISC-approved procedural requirements, characterized as privacy safeguards by the *Muhtorov* court, also favored finding any incidental collection reasonable.[187] As such, these courts all saw Section 702-derived intelligence collection as reasonable under the Fourth Amendment.

180. *Muhtorov*, 20 F.4th at 603–04; *Hasbajrami*, 945 F.3d at 666–67; *Mohamud*, 843 F.3d at 441–42; *In re Directives*, 551 F.3d at 1012, 1016.

181. 843 F.3d at 442. *But see* United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010) (concluding, in a non-foreign-intelligence context, that internet service providers are like post offices or telephone companies, rather than typical third parties, and therefore the government must still obtain a warrant to compel internet service providers to turn over subscriber information).

182. 945 F.3d at 663–64, 667.

183. 20 F.4th at 597–99.

184. Warrantless searches and seizures permitted under the plain-view doctrine require that (1) the seizing official be lawfully present at the location of seizure, (2) the official have proper access to the item seized, and (3) the item seized be obviously incriminating. *Id.* at 597 (citing United States v. Castorena-Jaime, 285 F.3d 916, 924 (10th Cir. 2002)).

185. *Id.* at 598–99. Interestingly, the argument here that two-way communication with a surveilled target necessitates lawful access to incidental communications appears functionally equivalent to an argument based on the third-party doctrine. The difference between the two seems to be the frame of reference. The first argument is from the government's perspective, while the second argument is from the individual target's perspective.

186. *See id.* at 580–81 (describing how the defendant supported and planned to join a terrorist organization).

187. *Id.* at 603–04; *see also* United States v. Mohamud, 843 F.3d 420, 443–44 (9th Cir. 2016) (finding that the Section 702 procedures adequately protected the defendant's privacy interest).

B. Post-Collection Querying and the Fourth Amendment

As for post-collection querying, only the Second Circuit in *Hasbajrami*[188] and the FISC in its annual Section 702 certification opinions have considered how it interacts with the Fourth Amendment. The *Hasbajrami* court reasoned that any U.S.-person query should constitute "a Fourth Amendment event . . . requiring the query itself be reasonable" and suggested that these queries could require warrants.[189] On the other hand, the FISC has regularly disagreed. It has consistently held that U.S.-person querying does not require additional Fourth Amendment scrutiny and is constitutionally reasonable under the totality-of-the-circumstances balancing test.[190] This Note argues that the FISC's approach has a stronger basis than the Second Circuit's, taking a more comprehensive view of Section 702.

1. An Anti-Programmatic Approach to Reasonableness.—The Second Circuit in *Hasbajrami* reasoned that Section 702 queries each constitute an independent constitutional event, therefore requiring additional Fourth Amendment scrutiny.[191] It explained that such a requirement would guard U.S. persons' privacy interests and guarantee that they "are not being improperly

188. The Second Circuit ultimately remanded the post-collection querying for the district court to investigate. United States v. Hasbajrami, 945 F.3d 641, 675–77 (2d Cir. 2019). On February 10, 2025, the Eastern District of New York ruled in a non-precedential and heavily redacted slip opinion that the government violated the Fourth Amendment when it conducted post-collection querying. United States v. Hasbajrami, No. 1:11-CR-623, 2025 WL 447498, at *19 (E.D.N.Y. Feb. 10, 2025). However, the district court's analysis is likely to be fundamentally flawed. *See* George Croner, *EDNY Opinion in Hasbajrami Undermines FISA 702*, LAWFARE (Mar. 31, 2025), https://www.lawfaremedia.org/article/edny-opinion-in-hasbajrami-undermines-fisa-702 [https://perma.cc/GBT7-APT3] (arguing that the court's approach was mistaken). Furthermore, the court appeared to significantly deviate from the Second Circuit's analytical approach. *Id.* This Note is primarily concerned with that approach and as such will focus on it rather than the contentious, though more recent, district court opinion.

189. *See Hasbajrami*, 945 F.3d at 672–73 (finding that individual queries each require a Fourth Amendment analysis but declining to determine whether this means U.S.-person queries require warrants). *But see* Adams, *supra* note 114, at 447–48 (suggesting that U.S.-person queries likely, but do not necessarily, fall under the foreign intelligence exception to the warrant requirement); Emily Berman, *When Database Queries Are Fourth Amendment Searches*, 102 MINN. L. REV. 577, 603–04 (2017) ("[T]he conventional wisdom is that once data is in the government's hands, the Constitution has nothing to say at all. In the words of one respected jurist, 'the [F]ourth [A]mendment does not control how properly collected information is deployed.'" (quoting Green v. Berge, 354 F.3d 675, 680 (7th Cir. 2004) (Easterbrook, J., concurring) (other citations omitted))).

190. *E.g.*, 2024 FISC Opinion, *supra* note 81, at 29–32; *accord supra* note 189 (listing some additional sources supporting the FISC's position).

191. *Hasbajrami*, 945 F.3d at 672.

targeted."[192] The court relied on four points in its reasoning,[193] the first two of which remain relevant today.[194]

First, it noted that recent cases outside the surveillance context support requiring additional Fourth Amendment reasonableness or probable cause inquiries despite otherwise lawful searches or seizures.[195] The Second Circuit pointed to cases where the government lawfully seized but improperly searched personal computing devices like cell phones,[196] computers,[197] and storage disks.[198] In these cases, the government should have obtained an additional warrant to search the devices despite their lawful seizure.[199]

Second, the Second Circuit highlighted what it perceived as the peculiarly large scale of Section 702 surveillance capabilities.[200] The court acknowledged that incidental collection might evoke the incidental-overhear or plain-view doctrines, suggesting the collection and use are reasonable.[201] However, the court distinguished Section 702 incidental collection from the typical incidental-overhear or plain-view case.[202] Incidental seizures typically occur contemporaneously with the underlying lawful seizure, but the volume of data that Section 702 programs collect suggests that any search of the collected material would be temporally decoupled from its lawful seizure.[203]

---

192. *Id.*

193. The court's reasoning was "based on three considerations," but it added a fourth qualification amounting to an additional reason of its own. *Id.* at 670, 672.

194. On point three, the Second Circuit speculated about the possibility of law enforcement conducting unreasonable queries against an ever-expanding pool of incidentally collected data, *id.* at 672, but recent amendments to FISA have greatly attenuated, if not mooted, these concerns. *See supra* notes 162–64 and accompanying text (listing changes to the contemporary Section 702 regime as it pertains to FBI querying procedures). On point four, the Second Circuit worried about improper querying across different agency databases, *Hasbajrami*, 945 F.3d at 672–73, but the information publicly available today on agencies' various targeting, minimization, and querying procedures and infrastructure cuts against this concern. *See supra* subpart II(B).

195. *Hasbajrami*, 945 F.3d at 670–71.

196. *Id.* at 670 (citing Riley v. California, 573 U.S. 373, 401 (2014)).

197. *Id.* at 670–71 (citing United States v. Sedaghaty, 728 F.3d 885, 912–13 (9th Cir. 2013)).

198. *Id.* at 671 (citing United States v. Runyan, 275 F.3d 449, 464–65 (5th Cir. 2001)).

199. *See Riley*, 573 U.S. at 401 (holding that a warrant is generally required to search a cell phone lawfully seized incident to arrest); *Sedaghaty*, 728 F.3d at 913 (holding that a new warrant was required to search lawfully seized items beyond what was authorized by the original warrant); *Runyan*, 275 F.3d at 464 (finding that police's pre-warrant search exceeded the scope of a prior private search and therefore any evidence obtained is likely subject to suppression).

200. *Hasbajrami*, 945 F.3d at 671.

201. *Id.*

202. *Id.*

203. The Second Circuit cited the Privacy and Civil Liberties Oversight Board's estimation that Section 702 downstream collection was acquiring almost 250 million emails annually by 2011 and likely more since then, suggesting that those emails are not being reviewed contemporaneously. *Id.* (citation omitted).

The *Hasbajrami* court considered this decoupling disconcerting when paired with the scale of the incidentally collected materials.[204] The court found support in *Riley v. California*[205] and *Carpenter v. United States*,[206] two Supreme Court decisions regarding searches of digital data.[207] The Second Circuit noted parallels between large-scale Section 702 collection and the vastness and breadth of the searched data in those cases, which were emphasized by the Supreme Court in its opinions.[208] The Second Circuit quoted the *Riley* Court's concern about cell phones placing "vast quantities of personal information literally in the hands of individuals."[209] It pointed to similar language in *Carpenter*, where the Supreme Court held that accessing cell-site location data via a third party constituted a search.[210] In *Carpenter*, the Supreme Court saw the "depth, breadth, and comprehensive reach" of the searched data and the "inescapable and automatic nature of its collection" as eliciting Fourth Amendment protection.[211] Accordingly, the Second Circuit signaled that the scope of Section 702 collection may raise Fourth Amendment concerns akin to those recognized in *Riley* and *Carpenter*.

2. Reasonableness, the Totality of Circumstances, and Querying.—The FISCR has not decided whether post-collection queries of Section 702 data require an individualized Fourth Amendment inquiry,[212] but the FISC has.[213] In its 2024 Memorandum Opinion and Order, the FISC found that post-collection U.S.-person queries were constitutionally reasonable given the constraints imposed by each agency's targeting, minimization, and querying procedures.[214] In contrast to the Second Circuit, the court expressly stated that these queries do not constitute individual Fourth Amendment events.[215] The FISC instead applied the totality-of-the-circumstances balancing test and found that the

204. *See id.* ("If such a vast body of information is simply stored in a database, available for review by request from domestic law enforcement agencies . . . , the program begins to look more like a dragnet, and a query more like a general warrant . . . .").

205. 573 U.S. 373 (2014).

206. 138 S. Ct. 2206 (2018).

207. *Hasbajrami*, 945 F.3d at 671–72.

208. *See id.* (exemplifying the Fourth Amendment implications of the government's newfound technological abilities as encapsulated by the comprehensiveness of these abilities' reach).

209. *Id.* at 671 (quoting *Riley*, 573 U.S. at 386).

210. *Id.* at 671–72 (quoting *Carpenter*, 138 S. Ct. at 2223).

211. *Id.* (quoting *Carpenter*, 138 S. Ct. at 2223).

212. The closest the FISCR got to deciding this issue was in *In re DNI/AG 702(h) Certifications 2018*, 941 F.3d 547, 563–64 (F.I.S.C.R. 2019). However, it did not need to reach the issue and left the question for the FISC to resolve. *Id.* at 565–66.

213. *E.g.*, Document re: Section 702 2021 Certification, Mem. Op. & Order, at 64–66 (F.I.S.C. Apr. 21, 2022) (determining, despite *Hasbajrami*, that per-query reasonableness inquiries were not necessary given the reasonableness of procedural constraints on the government as determined by a totality-of-the-circumstances balancing test).

214. 2024 FISC Opinion, *supra* note 81, at 32.

215. *Id.* at 28–29.

government's national security interest outweighed individual privacy concerns.[216] On the government-interest side of the balance, the FISC noted that national security, and consequently foreign intelligence, is a "particularly intense [governmental] interest."[217]

On the individual-privacy side of the balance, the FISC found that the querying procedures, "in the context of the entirety of the Section 702 program," significantly attenuated individual privacy concerns.[218] Looking at Section 702 as a whole, the court walked through the statutory protections afforded by all three sets of procedures.[219] Targeting procedures constitute the primary foundational safeguard for individual privacy. From the outset, these targeting procedures concentrate surveillance efforts on non-U.S. persons abroad who reasonably relate to a foreign intelligence purpose.[220] As such, the pool of data available to query is necessarily bounded by a bias towards national security matters.[221] Minimization procedures further reduce this pool, deleting or obscuring irrelevant U.S.-person information upon its discovery.[222] And finally, querying procedures reimpose a foreign intelligence purpose on any query submitted.[223]

Taking a view of querying in this broader context, an analyst performing a U.S.-person query can only do so for some foreign intelligence purpose. The query searches through a dataset that is itself biased towards foreign intelligence matters. And any irrelevant information will typically be deleted or redacted. Given these limitations, the FISC determined that Section 702 provided significant protections for individual privacy without requiring additional Fourth Amendment inquiries for each query.[224] The government's

---

216. *Id.* at 29.

217. *Id.* at 26 (quoting *In re* Certified Question of Law, 858 F.3d 591, 606 (F.I.S.C.R. 2016) (internal quotation marks omitted)); *see also In re Certified*, 858 F.3d at 608 (quoting Haig v. Agee, 453 U.S. 280, 307 (1981)) ("'[N]o governmental interest is more compelling' than national security.").

218. 2024 FISC Opinion, *supra* note 81, at 29–31.

219. *Id.* at 24, 26–31.

220. *See supra* section II(B)(1) for a more detailed description of the targeting procedures.

221. *See* 2024 FISC Opinion, *supra* note 81, at 31 (walking through these procedures with an eye towards FBI U.S.-person queries in particular).

222. *Id.* at 28.

223. *Id.* at 29; *see also* 2023 FISC Opinion, *supra* note 157, at 75 ("Although human examination of the private communications of persons protected by the Fourth Amendment involves a substantial intrusion, such examination is reasonable when the communications were properly acquired under Section 702 and returned by a query satisfying the 'reasonably likely to retrieve' standard." (citation omitted)).

224. 2024 FISC Opinion, *supra* note 81, at 28–29, 32; *see also* David E. Pozen, *Privacy-Privacy Tradeoffs*, 83 U. CHI. L. REV. 221, 240 (2016) ("[T]he suggested tradeoff is that tighter limits on what sorts of data the NSA can electronically collect or mine at the front end might lead to looser—and more privacy-invasive—investigatory practices at the back end."). The FISC's reasoning here is reminiscent of a softened version of the Supreme Court's analysis of the Fourth Amendment reasonableness of a drug-sniffing dog in *Illinois v. Caballes*, 543 U.S. 405, 407–10 (2005). Just as

interest thus held sway, and the FISC found Section 702's targeting, minimization, and querying procedures together to be reasonable under the Fourth Amendment.[225]

3. Comparing the Second Circuit and FISC's Approaches.—The Second Circuit, unlike the FISC, did not incorporate Section 702's procedural constraints into its reasoning as to why a U.S.-person query warranted an additional reasonableness inquiry, making its analysis less persuasive. The court's first consideration centered on cases requiring an additional warrant to search lawfully seized technological devices.[226] These items, like cell phones and computers, often contain within themselves the whole of a person's life down to the most intimate detail.[227] In contrast, U.S.-person information incidentally collected under Section 702 is unlikely to be so wide-ranging in scope. Section 702's targeting procedures constrain the government to surveilling non-U.S. persons for foreign intelligence purposes.[228] This singular purpose limits the results of U.S.-person queries to a far narrower slice of life than the results of phone or computer searches would be.[229]

The Second Circuit's second consideration focused on the large scale of Section 702 surveillance programs and analogized it to the vastness of the digital data at issue in *Riley* and *Carpenter*.[230] But as mentioned, the limited purpose of Section 702 collection nontrivially restricts the content of that collection, however large it may be. The breadth discussed in *Riley* and *Carpenter* speaks to the nature of the privacy interest, not merely the volume of data itself. While searching through a phone can readily reveal the whole of a person's life, searching through U.S.-person communications incidentally collected in the pursuit of foreign intelligence likely will not.

---

a drug dog is constrained to detecting drugs, the FISC viewed the Section 702 analyst as similarly constrained to detecting foreign intelligence. *Cf.* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 535 (2007) (noting the *Caballes* Court's reasoning that a drug dog is constrained to alerting to the presence of drugs and only drugs, and therefore its use does not violate any reasonable expectation of privacy).

225. 2024 FISC Opinion, *supra* note 81, at 32; *see also* Adams, *supra* note 114, at 443–46 (focusing on existing minimization procedures and traditional law enforcement precedent—instead of the combination of targeting, minimization, and querying procedures—as favoring a reasonableness determination).

226. United States v. Hasbajrami, 945 F.3d 641, 670–71 (2d Cir. 2019) (citing Riley v. California, 573 U.S. 373, 401 (2014); United States v. Sedaghaty, 728 F.3d 885, 912–13 (9th Cir. 2013); and United States v. Runyan, 275 F.3d 449, 464 (5th Cir. 2001)).

227. *See Riley*, 573 U.S. at 403 (discussing how cell phones often hold "the privacies of life" (citation omitted)).

228. *See supra* notes 124–33 and accompanying text.

229. *See* 2024 FISC Opinion, *supra* note 81, at 31 (noting that the likelihood of successfully querying for non-foreign-intelligence-related evidence of a crime is probably low given the constraints imposed by Section 702 targeting procedures).

230. *Hasbajrami*, 945 F.3d at 671.

Thus, the FISC's approach to post-collection querying correctly advances Section 702's procedural constraints as the likely lynchpin of any comprehensive Fourth Amendment analysis of Section 702 surveillance programs. This focus on procedural limitations can also alleviate fears of overly broad data collection, heedless handling of U.S.-person data, and improper purpose in reviewing this data.

IV. New Tech, Old Rules?

The FISC recently approved Section 702 procedures featuring automated processes for the NSA and CIA. In approving these automated processes, the court also effectively required a human analyst be the one to initiate and justify queries. This human-in-the-loop requirement stems less from any normative benefit to human participation and more from the statutory requirements of Section 702. In particular, the requirement for *ex ante*, fact-based justifications for any Section 702 query is likely difficult for current artificial intelligence systems to satisfy without first accessing protected information.

The distinction between permissible automated processing and impermissible automated querying lies with a threshold question of human observability. Actions that, of their own accord, render otherwise private information observable to others warrant higher constitutional and statutory scrutiny. However, automated processes that merely serve as an intermediate step for human-initiated surveillance actions like querying do not.

A. Section 702 and Automated Processing

The FISC recently approved revisions to the NSA's and CIA's Section 702 procedures that introduced automated processes and tools for the first time. The court found the changes to be statutorily and constitutionally valid, basing its reasoning on a retrieval-centric view of queries that pinned privacy concerns to the point of inspection or affirmative use.

1. 2023 NSA Automated Processing Procedures and FISC Approval.—In 2023, the NSA updated its querying and minimization procedures.[231] Novel automated capabilities figured prominently in these changes.[232] The new querying and minimization procedures redefined the term "processing" and then excluded "processing" from its definition of query.[233] The FISC reviewed

231. 2023 FISC Opinion, *supra* note 157, at 29.

232. *Id.* at 38–39, 54.

233. *Contrast* 2023 NSA MINIMIZATION PROCEDURES, *supra* note 151, at 4 (containing the new processing definition), *and* 2023 NSA QUERYING PROCEDURES, *supra* note 156, at 2–3 (containing the new processing and querying definitions), *with* NAT'L SEC. AGENCY, MINIMIZATION PROCEDURES USED IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION 4 (2022), https://www.intel.gov/assets/documents/702%20

these changes and found that they complied with both Section 702's statutory requirements and the Fourth Amendment's reasonableness requirements.[234]

The NSA's updated minimization and querying procedures redefined process or processing to mean:

> [A]ny action necessary to convert unminimized Section 702-acquired information into an intelligible form or any machine-initiated action designed to identify, curate, label, or organize such information; provided, however, that the term "process" or "processing" does not include an action that: (1) presents information for human inspection; or (2) using means that do not involve human inspection, produces and makes affirmative use of information for investigative, intelligence analysis, or preventative purposes.[235]

The 2023 querying procedures, mirroring Section 702's language, defined query as "the use of one or more terms to retrieve the unminimized contents or noncontents . . . of Section 702-acquired information."[236] However, this definition excluded "activities that constitute the processing of unminimized Section 702-acquired information."[237] The "processing" exemption is absent from the language of Section 702, thereby creating potential for foreign intelligence analysis to occur outside its statutory bounds.[238]

Nevertheless, the FISC found that these changes complied with Section 702.[239] The court noted that "processing" expressly excludes, and thus "querying" can still include, automated actions that retrieve unminimized information for human use or make affirmative use of that information themselves.[240] The FISC concluded that these redefined terms were statutorily compliant because automated actions that trigger privacy concerns were still subject to standard querying and minimization rules.[241]

Looking to the statutory meaning of query, the court emphasized the act of retrieval as a core and inseparable characteristic of any query.[242] The court

---

Documents/declassified/21/2021_NSA_Minimization_Procedures-Amended.pdf [https://perma.cc/Z8HN-NKWE] (lacking the changes), *and* NAT'L SEC. AGENCY, QUERYING PROCEDURES USED IN CONNECTION WITH ACQUISITIONS OF FOREIGN INTELLIGENCE INFORMATION 1–2 (2022), https://www.intelligence.gov/assets/documents/702%20Documents/declassified/21/2021_NSA_Querying_Procedures-Amended.pdf [https://perma.cc/ZE9V-VE99] (same).

234. 2023 FISC Opinion, *supra* note 157, at 67, 81.

235. 2023 NSA MINIMIZATION PROCEDURES, *supra* note 151, at 4; 2023 NSA QUERYING PROCEDURES, *supra* note 156, at 2.

236. 2023 NSA QUERYING PROCEDURES, *supra* note 156, at 2; 50 U.S.C. § 1881a(f)(5)(B).

237. 2023 NSA QUERYING PROCEDURES, *supra* note 156, at 2.

238. *See* 50 U.S.C. § 1881a(f)(5)(B) (lacking this processing exception).

239. 2023 FISC Opinion, *supra* note 157, at 40.

240. *Id.* (quoting 2023 NSA QUERYING PROCEDURES, *supra* note 233, at 2).

241. *Id.*

242. *See id.* at 41 (noting that the act of retrieval cannot be separated from a query).

elaborated that everything in the chain from a query's constituent terms to information retrieval constitutes a single procedural action.[243] The FISC also noted Section 702's overarching goal of protecting U.S. persons from unreasonable invasions of privacy.[244] Combining the statutory meaning of "query" with this broader purpose, the FISC reasoned that privacy concerns only arise when U.S.-person information is divulged or otherwise put to affirmative use.[245] Thus, in the surveillance context, it is the act of inspecting or analyzing retrieved unminimized information that triggers privacy concerns.[246] Whether the inspector is a human analyst or an automated algorithm makes no difference.[247] In contrast, automated processing that merely transforms raw and unminimized data into "queryable forms" does not elicit these concerns.[248] This unminimized, but now queryable, information remains inert until later retrieved and used for some governmental purpose.[249]

The FISC similarly analyzed a classified NSA system that automatically generates smaller datasets from a larger pool of unminimized collection data.[250] The court found that the system's operations were not queries, describing them as "machine-initiated actions" that neither retrieved information for human inspection nor made affirmative use of that information.[251] To access the datasets this classified system created, NSA analysts still needed to submit queries pursuant to the NSA's general querying procedures.[252] Additionally, the smaller datasets were less likely to contain U.S.-person information than the broader datasets from which they were drawn.[253] As such, the FISC found that this kind of automated action did not amount to a meaningful intrusion of privacy.[254]

The FISC also found that excluding "processing" actions from the standard querying definition did not raise meaningful Fourth Amendment concerns.[255] The court applied the usual totality-of-the-circumstances

243. *Id.* at 42–43 (citing 2023 NSA QUERYING PROCEDURES, *supra* note 233, at 2).

244. *Id.* at 38; *see, e.g.*, 50 U.S.C. § 1881a(f)(1)(A) (mandating that querying procedures be consistent with the Fourth Amendment and hence serve to protect U.S.-person privacy interests).

245. *See* 2023 FISC Opinion, *supra* note 157, at 38–39 (concluding that merely converting Section 702-acquired data into queryable forms does not meaningfully infringe on U.S. persons' privacy).

246. *Id.*

247. *See id.* at 39–40 (describing human and machine querying as similarly able to negatively impact U.S. persons).

248. *Id.* at 38–39.

249. *Id.* at 39.

250. *Id.* at 65–66.

251. *Id.* at 64.

252. *Id.*

253. *Id.* at 65.

254. *Id.* at 65–66.

255. *Id.* at 75–76.

balancing test to make this Fourth Amendment reasonableness determination. On the privacy-intrusion side, the court understood processing actions, which never review information themselves, to be minimally intrusive as compared to human review.[256] The court even found that processing actions may increase privacy protections for individuals.[257] And on the governmental-interest side, the FISC found that processing actions advance the government's strong interest in foreign intelligence.[258] Thus, the court found processing actions, and any automated actions that qualify as processing, to be reasonable under the Fourth Amendment.[259]

2. 2024 CIA Automated Processing Tool and FISC Approval.—In 2024, the FISC considered a classified CIA system that automatically mines and processes Section 702 data upon receipt.[260] To retrieve this processed data, a CIA analyst must opt in to using this system when submitting a query.[261] If so enabled, the system only returns information related to the query's terms.[262] The court found this system to be both statutorily compliant with Section 702 and constitutionally reasonable under the Fourth Amendment.[263]

The FISC considered this automated system substantially similar to the NSA processing actions it considered in 2023.[264] Like the NSA, the CIA's querying procedures define query as "the use of one or more terms to retrieve the unminimized contents or noncontents of Section 702-acquired information."[265] Unlike the NSA, the CIA procedures do not provide for processing actions that are distinct from general queries.[266] However, the CIA's automated system would qualify as processing under both the NSA's definition, and the FISC's interpretation, of the term.[267]

Given these similarities, the FISC extended its reasoning regarding NSA processing actions to the CIA's new automated querying system. It found the CIA system statutorily compliant because it never retrieves data absent an analyst's procedurally compliant query.[268] The FISC also found the

256. *Id.* at 75.

257. *Id.* at 76.

258. *Id.*

259. *Id.* at 81.

260. *See supra* notes 81–84 and accompanying text.

261. *See id.* at 32–33 (noting that the system is an "optional feature").

262. *Id.* at 33.

263. *Id.* at 35–36.

264. *Id.* at 35.

265. 2019 CIA QUERYING PROCEDURES, *supra* note 158, at 2.

266. *Contrast* 2024 CIA QUERYING PROCEDURES, *supra* note 158, at 1–2 (lacking a definition for process or processing), *with* 2024 NSA QUERYING PROCEDURES, *supra* note 156, at 2 (containing a definition for process and processing).

267. 2024 FISC Opinion, *supra* note 81, at 35.

268. *Id.*

CIA system constitutionally reasonable. The strong governmental interest in foreign intelligence, bolstered by the CIA tool, outweighed individual privacy concerns, which the court viewed as minimal given the tool's autonomous nature.[269]

An automated action thus lives and dies by its status as a query or a non-query. An automated query, like any other query, must comply with Section 702's querying procedures.[270] These procedures mandate that any query have a foreign intelligence purpose and that the determination of this purpose be backed up by some fact-based explanation.[271] Crucially, these are *ex ante* determinations made before the analyst accesses a Section 702 database.[272] The NSA and CIA's automated processing actions do not impinge on these *ex ante* obligations and are hence minimally problematic, if at all.

B. Schrödinger's Robot: Automating Fourth Amendment Reasonableness

This kind of automation figures into any Fourth Amendment reasonableness analysis. The FISC concluded that the NSA and CIA's automated processing actions that were not queries were reasonable under the Fourth Amendment.[273] The court found any privacy impact wrought by automated processing to be less than that of human review.[274] But it did not elaborate as to why and did not reach the question of how automated queries influence reasonableness determinations.[275]

This Note posits that the concept of human observability fills this gap. A critical threshold question for any automated system is whether it renders protected information observable. Systems that do so should receive increased legal scrutiny, but those that do not should not receive increased scrutiny. The automated processes that the FISC approved fall into this second category. These processes were intermediate steps that could not—by themselves and without human initiation—make protected information observable. As such, their inclusion in the NSA and CIA's Section 702 procedures should not and did not render those procedures constitutionally or statutorily invalid.

---

269. *Id.* at 35–36.

270. *See* 2023 FISC Opinion, *supra* note 157, at 39–40 (analogizing automated querying to standard human querying).

271. *See supra* note 158 and accompanying text.

272. *See supra* note 158 and accompanying text.

273. 2024 FISC Opinion, *supra* note 81, at 35–36.

274. *Id.*

275. The court has discussed queries in the travel-vetting context, but those queries are different from standard Section 702 queries and are not discussed in this Note. *Supra* note 157.

1. Analysts in the Loop.—The practical consequence of the FISC's discomfort with machine-initiated automated queries is to mandate human involvement in affirmative uses of Section 702 data.[276] In other words, the FISC imputes a human in the loop for Section 702 surveillance. This human-in-the-loop constraint, however, has less to do with the possible benefits of human involvement and more to do with the substantial limits Section 702 places on agency discretion.

The idea of a "human in the loop," at its broadest, spans all scenarios where a human works with some automated system when executing a decision.[277] Requiring humans in the loop can serve multiple purposes.[278] Most relevant to the Section 702 context, human analysts could, ideally, play a justificatory role,[279] an accountability role,[280] or a dignitary role.[281] However, each of these roles is undermined by the difficulties in predicting the decisions of current artificial intelligence technologies.[282] Furthermore, the FISC did not meaningfully engage with these normative concepts in reaching its decision.

The FISC did wrestle with the statutory constraints imposed by Section 702. In harmonizing Section 702's requirements with the automated processes at issue, the FISC effectively prohibited wholly automated actions from performing query functions and thus implicitly required human analysts to perform queries. The FISC's prohibition of automated queries arises out of Section 702's requirement that each query have an *ex ante* and fact-based justification prior to submission.[283] Analysts must explain how their query serves a proper foreign intelligence purpose.[284] This limit on their discretion exists in service of protecting U.S.-person privacy interests.[285] It also renders current cutting-edge artificial intelligence technologies unable to comply

276. *Cf.* Aziz Z. Huq, *A Right to a Human Decision*, 106 VA. L. REV. 611, 627 (2020) (explaining how statutory and constitutional structures can mandate human—rather than machine—involvement by implication).

277. Rebecca Crootof, Margot E. Kaminski & W. Nicholson Price II, *Humans in the Loop*, 76 VAND. L. REV. 429, 440 (2023).

278. *Id.* at 473–74 (listing corrective, resilience, justificatory, dignitary, accountability, "stand-in," friction, "warm body," and interface roles).

279. In a justificatory role, an analyst would provide reasons for an algorithm's decision. *Id.* at 473.

280. In an accountability role, an analyst would be held responsible for algorithmic decisions. *Id.*

281. In a dignitary role, an analyst would aim to protect the dignity of surveilled U.S. persons. *Id.*

282. *See supra* notes 47–49 and accompanying text.

283. *See supra* notes 271–72 and accompanying text.

284. *See supra* note 271 and accompanying text.

285. *Cf.* Emily Berman, *A Government of Laws and Not of Machines*, 98 BOS. U.L. REV. 1277, 1342 (2018) (describing the usual reasons for such limits on government discretion, including the protection of Fourth Amendment privacy rights).

unless they can give such *ex ante* reasons without first accessing a protected database.[286]

2. Is Observation All You Need?—In approving the NSA and CIA processing revisions, the FISC anticipated Professor Orin Kerr's insight on human observability and digital searches.[287] Professor Kerr notes that relevant Supreme Court jurisprudence ties privacy intrusions to human observation.[288] Albeit in a slightly different technological context, he argues that the whole chain of information retrieval—from query to database search to output—should inform a search's Fourth Amendment validity.[289] This validity, in turn, hinges on when protected or private information is exposed to human observation.[290] However, Professor Kerr wholly exempts artificial-intelligence-based queries from his analysis due to concerns about the black-box nature of the technology.[291] Despite this black box, this section argues that observability should remain the critical threshold factor for determining the reasonableness of artificial-intelligence-based querying in the context of Section 702 surveillance.

Automated querying's impact on Fourth Amendment reasonableness depends on whether a computer or artificial-intelligence system can, by itself, intrude on someone's privacy in the first place. This threshold question remains unresolved, but the weight of legal scholarship today considers computers incapable of intruding upon privacy on their own.[292] Proponents of this position explain that any intrusion of privacy depends on the exposure of private information to another human.[293] As such, any privacy harms resulting from computer review ultimately must be realized by some human actor.[294] Fourth Amendment privacy intrusions rest not on computer or

286. However, in such environments, machine learning solutions are less likely to be useful anyway. *See id.* at 1343–45 (describing the limits of these models in low-discretion regulatory environments).

287. *See* Kerr, *supra* note 154, at 5 (arguing for a "filter-focused approach to data scanning" that emphasizes the facts that were explicitly or implicitly revealed from data).

288. *Id.* at 32.

289. *Id.* at 35–36.

290. *Id.* at 49.

291. *Id.* at 47.

292. Jones, *supra* note 40, at 95–96; Crootof et al., *supra* note 277, at 457.

293. *E.g.*, Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 616 (2011).

294. Bruce E. Boyden, *Can a Computer Intercept Your Email?*, 34 CARDOZO L. REV. 669, 705 (2012); *see also* Tokson, *supra* note 293 ("The common element of the violations of privacy . . . is the exposure of ourselves or our information to another person, an observer capable of judging us and imposing social sanctions.").

automated action but instead on any resulting human conduct.[295] Thus, the arguments go, purely computerized actions themselves cannot constitute intrusions of privacy for Fourth Amendment purposes.[296] A stronger form of this argument requires that, for a privacy violation to occur, a computer must reveal private information to a human mediator.[297] A weaker form covers more general cases where purely automated actions interact with private information such that observable privacy harms result.[298]

The premise that real-world harms require a human mediator is likely unpersuasive. The FISC has found a human-free causal link between automation and harm to be a plausible concern that should not be ignored.[299] The court illustrated its worry with the example of an automated algorithm adding a U.S. person to a no-fly list, which obviously causes harm, without any human involvement.[300] Additionally, today's information environment often involves interpreting high volumes of varied information under severe time constraints,[301] which incentivizes purely machine-based decision making.[302] Accordingly, private actors in industries like high-frequency trading and content moderation regularly implement systems where automated actions impact people without a human involved.[303]

---

295. *See* Tokson, *supra* note 293, at 617 (arguing that automated computers alone cannot truly violate privacy interests); Boyden, *supra* note 294, at 673 ("[A] computer is, at most, a tool that enables humans to spy on other humans; it cannot *itself* spy on people.").

296. Tokson, *supra* note 293, at 617.

297. *See* Jones, *supra* note 40, at 94 (reading Supreme Court precedent to require human involvement for an invasion of someone's reasonable expectation of privacy to have occurred); Pozen, *supra* note 224, at 239–40 (citing Richard A. Posner, *Our Domestic Intelligence Crisis*, WASH. POST (Dec. 21, 2005), https://www.washingtonpost.com/wp-dyn/content/article/2005/12/20/AR2005122001053.html [https://perma.cc/L2S7-7SMP]) (describing Posner's argument that "machines cannot by themselves invade privacy; only other humans can"); *cf.* 2023 FISC Opinion, *supra* note 157, at 39 (acknowledging that in the context of Section 702, Congress "focused on human inspection as a point at which substantial intrusion on Fourth Amendment-protected interests may occur").

298. *Cf.* 2023 FISC Opinion, *supra* note 157, at 39–40 (noting that, despite Congress's focus on human inspection in Section 702, purely automated actions could harm individuals' interests); Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 489–91 (2006) (introducing various privacy harms, many of which simply make private information more accessible to others).

299. *See* 2023 FISC Opinion, *supra* note 157, at 39–40 (finding that "automated analysis of private communications could, without human inspection, significantly disadvantage U.S. persons").

300. *Id.* It is worth noting that the harm of being on a no-fly list is not purely a privacy harm.

301. *See* Amir Gandomi & Murtaza Haider, *Beyond the Hype: Big Data Concepts, Methods, and Analytics*, 35 INT'L J. INFO. MGMT. 137, 140 (2015) (discussing the need to "turn high volumes of fast-moving and diverse data into meaningful insights"); Provost & Fawcett, *supra* note 42, at 51–52 (describing the vast volume and variety of data now available in every industry and the difficulties in processing and analyzing that data).

302. *See* Crootof et al., *supra* note 292, at 454–55 ("If there is a benefit to making decisions with superhuman speed, efficiency pressures discourage involving humans.").

303. *Id.* at 455.

However, this human-involvement theory can be generalized to a broader human-observer theory that applies even where automated actions cause real-world harms without any human involvement. Any problems with the human-involvement requirement need not be fatal to the broader theory. Instead, these issues describe the outer bounds of the special case where a person is in fact necessary to realize automated privacy intrusions.

The more generalized human-observer theory focuses on the distinction between information that is observable[304] and information that is unobservable. Only observable information can result in an intrusion of privacy.[305] Instead of viewing human *action* as necessary for any given privacy impact, the generalized theory views human *observability* as necessary for any given privacy impact. In the FISC's no-fly-list example, a privacy intrusion is possible because the automated process results in an action that can be observed, namely the U.S. person's addition to the no-fly list. When contained within an automated system, any information, processed or not, is unobservable and thus inert. However, when moved outside the automated system, that same information becomes observable and thus active.

Observability itself is not a marker of Fourth Amendment reasonableness. It is far too broad for that. At its core, observability merely describes a necessary requirement for something to warrant any constitutional or statutory consideration.[306] However, observability also changes the frame of reference from which to view an artificial intelligence system's black box. An observability-based analysis does not view black boxes as inscrutable agents acting as or among humans and instead focuses on the information contained inside.[307] The black box here becomes a separate sphere distinct from that of human affairs.

What is or happens inside this automated sphere is invisible, but its boundaries are permeable. Information can enter and leave, and actions that cause this movement are subject to constitutional scrutiny because they

304. By "observable," I mean to use a broad definition that includes "perceivable," "cognizable," or "interactable."

305. *See* Berman, *supra* note 189, at 619–20 ("Information about our spending or travel habits, or even the content of our Google chats, may be sitting on the government's servers, but nobody is looking at them . . . . [T]he moment government action becomes problematic is when it singles out an individual for scrutiny." (citations omitted)); Solove, *supra* note 298, at 506–23 (describing various processing actions that can result in harms when they involve observable information).

306. *See* Kerr, *supra* note 154, at 32 (deriving from Supreme Court precedent the principle that "[f]or a [Fourth Amendment] search to occur, information must be exposed to human observation"); *cf.* Berman, *supra* note 189, at 620 (asserting that "[o]ne cannot regulate the collection of data one cannot see" in the context of latent information that has yet to be processed into usable form).

307. *See* 2023 FISC Opinion, *supra* note 157, at 64 (distinguishing machine-initiated actions that merely "identify and organize" information from those that "present information for human inspection" or otherwise affirmatively use information); *cf. id.* at 38–39 (taking a similar information-focused approach in the statutory context).

transform the unobservable into the observable.[308] Much like how an energetic system can only gain or lose energy when subject to outside work,[309] an automated system can only gain or lose information when subject to some outside act.

The FISC considered information retrieval just such an act. Automated actions that provide data for human inspection or make affirmative use of such data also make the data observable, thus warranting increased review. These actions also qualify as queries. As such, agency querying procedures provide for this review and impose constraints burdensome enough to foreclose artificial intelligence from last-mile surveillance efforts under Section 702.

Conclusion

Section 702 seeks to protect U.S.-person privacy rights while preserving the government's interest in using the United States' vast electronic surveillance capacity against foreign intelligence targets. It does so by imposing procedural limits on intelligence agencies' discretion. However, the introduction of novel automated processes and actions adds new tensions to this system. Automated actions create the possibility of intruding on U.S.-person privacy without the reason-giving checks upon which Section 702's procedures rely. In response, the FISC interpreted the automated actions it thought most worrisome as constituting queries. Current technological limitations likely render artificial intelligence-based actions incompatible with Section 702's query requirements. Under this interpretation, artificial intelligence processes likely cannot extend past database server racks, and human analysts must remain the sole drivers of electronic surveillance efforts.

308. *See, e.g.*, 2024 FISC Opinion, *supra* note 81, at 26–27, 31–32 (citations omitted) (reviewing the Fourth Amendment reasonableness of targeting and collection procedures, which transfer information into the automated domain, and querying procedures, which transfer information out of the automated domain).

309. RANDALL D. KNIGHT, PHYSICS FOR SCIENTISTS AND ENGINEERS: A STRATEGIC APPROACH 279–80, 301 (3d ed. 2013).