The Hidden Kraken: Submarine Internet Cables and Privacy Protections

Christopher Guay

Table of Contents

I. Introduction

Beyond the existential dread associated with the greatest depths of the oceans, there rests one of the most important components to our modern civilization. No, it's not the eldritch horrors of the deep, it's instead the backbone of the internet. Underwater sea cables represent over "95 percent" of international communications traffic.[1] Underwater sea cables are key to how our modern internet connects the world. These cables allow communications from one country to reach another. Instead of relying upon satellites or radio technology, there are physical fiberoptic lines which connect landmasses of the world. That is why someone in the United States can access a British or German website without any major difficulty. At its core, submarine internet cables allow enormous amounts of commerce and communications to occur almost instantaneously.[2] Ultimately, the regulatory structure in the United States offers both significant benefits and significant dangers on the issue of information privacy.

There are two major issues related to submarine internet cables, one being related to government use of data and the other having to do with corporate use of data. On the first issue, the United States has accessed and surveilled these submarine internet cables.[3] On the second issue, in the United States, there does not appear to be any regulations stopping submarine cable operators from monetizing the information that goes through their cables. This results from a lack of a comprehensive set of privacy regulations similar to the General Data Protection Regulation (GDPR) in the European Union[4] or California's California Consumer Privacy Act (CCPA/CPRA).[5] The lack of comprehensive privacy regulations allow companies and the

[1] MICK GREEN ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD, 3 (2009).
[2] DEBORAH BARTLETT-MCNEILL., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD, 16 (2009).
[3] Olga Khazan, *The Creepy, Long-Standing Practice of Undersea Cable Tapping*, THE ATLANTIC, (July 16, 2013), https://www.theatlantic.com/international/archive/2013/07/the-creepy-long-standing-practice-of-undersea-cable-tapping/277855/.
[4] Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation (GDPR).
[5] Cal. Civ. Code §§ 1798.100-1798.199.100 (CCPA amended by CPRA ballot initiative).

government to collect vast amounts of data.[6] Advertising is big business, with a lot of money involved.[7] The global digital advertising industry is estimated to have $438 billion in revenue in 2021.[8]

While the current regulatory structure concerning submarine internet cables presents significant issues, the same regulatory structure offers some solutions. On the issue of government surveillance of data through submarine internet cables, there are not any easy and realistic solutions.[9] The President could order less surveillance, yet this seems unlikely. The only realistic option for limiting government surveillance would necessitate changing the law. On the other hand, the existing statutory and regulatory structure could offer some solutions to corporate intrusion in private information.[10] The President's broad power under the Cable Landing License Act of 1921 could allow the President to effectively regulate submarine cable operators and other interested parties. Failing that, the FCC could try to engage in a reinterpretation of submarine cable operators as mandatory common carriers.[11]

Submarine internet cables affect so much of daily life, but very little attention is paid to them. The information carried by submarine internet cables carry affects nearly all facets of daily life, making our modern system of interconnectedness possible.[12] Any information that is carried from one country to another is subject to the use of submarine internet cables.[13] Any time an individual interacts with a computer system that operates on the internet, it's possible for an

[6] Thematic Intelligence, GlobalData (Mar. 1, 2022), https://www.globaldata.com/media/thematic-research/adtech-drive-internet-advertising-industry-1-trillion-2030-forecasts-globaldata/.
[7] *Id.*
[8] *Id.*
[9] United States v. United States Dist. Court for Eastern Dist. of Mich., So. Div., 407 U.S. 297, 317-18 (1972).
[10] Cable Landing License Act of 1921, ch. 12, 42 Stat. 8 (1921) (codified as amended 47 U.S.C. §§ 34-39).
[11] Communications Act of 1934, ch. 652, 48 stat. 1064 (codified as amended 47 U.S.C. ch. 5).
[12] BARTLETT-MCNEILL., *supra* note 2, at 16.
[13] BARTLETT-MCNEILL., *supra* note 2, at 16.

advertiser to gain information about your behavior which can be monetized.[14] Submarine internet cables are another avenue for data collection.

Pew Research Center conducted a survey of Americans in 2019 which examined American's thoughts on privacy.[15] In that survey, Pew Research found that 62 percent of Americans believe that it is not possible to go about their daily lives without companies collecting their data.[16] Similarly, 62 percent of Americans believe that it would be impossible to go about their daily lives without the government collecting their data.[17] At the same time, over 80 percent of Americans believe that they have very little or no control over their own data.[18] Additionally, 79 percent of Americans are very or somewhat concerned about how companies use their data, and 64 percent were very or somewhat concerned with how the government uses the data their personal data.[19]

This makes the right to privacy so important. Just as corporations and others have an interest in learning about individuals' characteristics and behaviors, individuals have a contrasting interest in keeping information away from others.[20] Since the founding of America,

[14] Thematic Intelligence, *supra* note 6.
[15] Brooke Auxer et al., *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information***,** PEW RESEARCH CENTER (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/.
[16] *Id.*
[17] *Id.*
[18] *Id.*
[19] *Id.*
[20] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890) ("The intensity and complexity of life, attendant upon advancing civilization, have rendered necessary some retreat from the world, and man, under the refining influence of culture, has become more sensitive to publicity, so that solitude and privacy have become more essential to the individual[.]").

the desire for privacy has been part of the fabric of the United States.[21] The right to privacy is represented in both the United States Constitution[22] and in the common law.[23]

In one the most famous examples of exploring the concept of privacy as a right, Samuel Warren and Louis Brandeis argued that a right to privacy has always existed in the background of the common law:[24]

> These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned or possessed — and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.[25]

Of course, the types of privacy injuries Samuel Warren and Louis Brandeis were concerned with had to do with overly invasive journalists,[26] rather than the typical concerns of Americans today. This does not take away from the importance of maintaining some amount of privacy in the daily lives of anyone who uses the internet. The fundamental concern for privacy resonates today, just as much, if not more, than it did 100 years ago.

Even beyond publication of private information that one would typically want kept

---

[21] Warren & Brandeis, *supra* note 19, at 196.
[22] *See e.g.* McIntyre v. Ohio Elections Com'n, 514 U.S. 334, 357 (1995) (suggesting that anonymity acts as a "shield from the tyranny of the majority,").
[23] Warren & Brandeis, *supra* note 19, at 206
[24] *Id.*
[25] *Id.* at 205.
[26] *Id.* at 195-96.

private, the Constitution is concerned with ensuring individuals maintain some forms of privacy.[27] The privacy interests the constitution is interested in can be split up into different types of privacy such as: informational privacy,[28] physical privacy,[29] intellectual privacy,[30] associational privacy,[31] and decisional privacy.[32] Even with the privacy protections found in the common law and in the Constitution, modern day life has made it difficult to avoid being surveilled by myriad companies seeking to serve you advertisements.[33]

The problem is that privacy interests clash with the potential and actual problems with the current regulatory structure of submarine internet cables in the United States. The first issue of the United States government tapping into submarine internet cables represents a massive problem when considering how it interacts with the data privacy protections granted to European Union citizens under the General Data Protection Regulation (GDPR) and the processing of personal data in countries outside of the European Union.[34] The ability for the United States government to collect internet communications has created a problem for businesses trying to

[27] *See* U.S. CONST. amends. I, IV, V, IX, XIV.
[28] *See e.g.* Whalen v. Roe, 429 U.S. 589, 605 (1977) (explicitly deciding not to determine whether there is a Constitutional right to the protection of information privacy and the disclosure of private information that has been collected).
[29] Carpenter v. U.S., 138 S. Ct. 2206, 2217 (2018) (holding that individuals hold a reasonable expectation of privacy of their location when using their cellphones).
[30] Stanley v. Georgia, 394 U.S. 557, 565 (1969) (holding that the ability to satisfy "intellectual and emotional needs in his private home," through pornographic material is protected by the First Amendment) ("If the First Amendment means anything, it means that a State has no business telling a man, sitting alone in his own house, what books he may read or what films he may watch. Our whole constitutional heritage rebels at the thought of giving government the power to control men's minds.").
[31] McIntyre v. Ohio Elections Com'n, 514 U.S. 334, 357 (1995) (holding that the ability to associate without interference by the government is part of the First Amendment).
[32] Griswold v. Connecticut, 381 U.S. 479, 486-86 (1965) (holding that the usage of contraception in privacy is protected under the right for individuals to make individual decisions for themselves).
[33] *See* Thematic Intelligence, *supra* note 6.
[34] Case C-311/18, *Data Prot. Comm'n v. Facebook Ir. Ltd.,* ECLI:EU:C:2020:559 ¶¶ 52-60 (Jul. 17, 2020) (Commonly known as "Schrems II") (Where an Austrian national filed a complaint that the U.S. did not provide adequate protections for data of EU citizens transferred to the U.S.).

work in both the United States and Europe as it suspended the easy transfer of personal data from the EU to the US.[35]

President Joe Biden signed a new executive order on October 7, 2022, to ameliorate the concerns in the European Union to the privacy rights of European citizens.[36] Whether this will be enough to satisfy the European Union Court of Justice's concerns about the privacy of European citizens is another question. Based upon the fact that the European Union Court of Justice has already invalidated two previous agreements between the United States and the European Union, it remains to be seen whether this will provide enough protections.

While this has huge ramifications for America's relationship with Europe, government surveillance does not only implicate foreign relationships. Individuals have a privacy interest in not being surveilled by the government in their normal activities. There are not a lot of stop the government from this type of surveillance.[37] Something more must be done to ensure that privacy rights are protected, and that economic interaction does not get disrupted due to these programs.

The second issue concerning the lack of regulatory regime limiting how submarine cable operators behave presents a potential problem for consumers. Laws like the California Consumer Privacy Act (CCPA/CPRA) and the General Data Protection Regulation (GDPR) in Europe make it more difficult for companies to monetize their access to data.[38] As it becomes more difficult to monetize data through previous methods of information gathering, it logically follows

---

[35] *Id.* at ¶¶ 198-202 (Invalidating the EU-US Privacy Shield agreement as not fulfilling Article 45(1) of the GDPR).
[36] Exec. Order No. 14086, 87 C.F.R. 62283 (2022); Mark Scott et al., *Biden signs executive order on EU-US data privacy agreement*, POLITICO (Oct. 7, 2022) https://www.politico.eu/article/joe-biden-data-privacy-agreement-executive-order-eu-us/ (The Biden administration appears to think that this will be more than enough protections to satisfy the concerns in the European Union).
[37] *See* United States v. United States Dist. Court for Eastern Dist. of Mich., So. Div., 407 U.S. 297, 317-18 (1972).
[38] Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation (GDPR); Cal.Civ Code §§ 1798.100-1798.199.100 (CCPA amended by CPRA ballot initiative).

that enterprising companies will find alternatives. Submarine cables could offer a potential avenue for this time of monetization behavior. The United States must act proactively to ensure that submarine internet cables remain neutral operators. At the very least, it appears that submarine cable operators have the capability to create sectioned off data connections that give other companies the ability to restrict access of specific types of data.[39]

In order to fully explore these two issues, this comment will lay out foundational information about submarine internet cables. Only by understanding the full picture of submarine internet cables can someone fully examine the modern-day issue of regulating their use. First, this comment will examine how this regulatory structure creates a regulatory blind-spot for intrusions into privacy. Second, this comment will explore the basic technology that powers our connections across the world. Third, this comment will explain some of the history of the development of modern-day submarine internet cables. Fourth, this comment will lay out the regulatory history of submarine cables in context of the United States. Fifth, this comment will show how the regulation has grown into the modern day in the United States. Sixth, this comment will lay out how submarine cables have historically been regulated in the international context. Seventh, this comment will explore the current regulatory structure in the international context. Lastly, this comment will explore how the current regulatory structure in the United States offers some potential solutions to privacy concerns related to submarine internet cables.

II. Submarine Cables and Information Privacy Blindspot

Before examining what the regulatory blindspots are in the United States in relation to information privacy and submarine cables, it is important to understand why information privacy

[39] SUBCABLEWORLD, AN INTERVIEW WITH IVO IVANOV, CHIEF EXECUTIVE OFFICER, DE-CIX INTERNATIONAL (https://www.subcableworld.com/newsfeed/fiber-optic-cables/a-dramatic-change-in-how-sea-cables-will-be-monetized) (last visited Nov. 18, 2022).

is so critical. Information privacy by itself is sometimes hard to defend as a goal.[40] Why should innocuous information about what types of websites you visit or who you talk to on the Internet be hidden from the wider world? People have nothing to lose from companies or the government learning what websites they visit or who they talk to, right? This is information privacy, and it can be incredibly important. The logic for allowing individuals to maintain some amount of privacy in this type of information is that it allows for uncorrupted thought.

Informational privacy makes it possible for the effective exchange of democratic ideals.[41] In essence, when outsiders view the behaviors of individuals that "[e]xamination chills experimentation with the unorthodox, the unpopular, and the merely unfinished."[42] This means that the mere act of observation changes the way people will act and think.[43] Consequently, some amount of information privacy is necessary in order to allow a democratic society to flourish.

Both the United States government and private companies collect and analyze information about individuals and their usage of the internet.[44] Deep-sea internet cables offer a uniquely challenging issue for the regulation of the government's surveillance of individuals.[45] At the same time, the regulatory structure of deep-sea internet cables in the United States offers a great chance to effectuate change through the entire industry. In addition, there is the fear that private owners of underwater internet cables can and do use the information that flows through their cables.[46]

A. Government Use

---

[40] Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52. Stan. L. Rev. 1373, 1375 (2000).
[41] *Id.* at 1426.
[42] *Id.*
[43] *Id.*
[44] Khazan, *supra* note 3; *See also*Thematic Intelligence, *supra* note 6.
[45] Khazan, *supra* note 3.
[46] James Griffiths, *The global internet is powered by vast undersea cables. But they're vulnerable.*, CNN, (July 26, 2019), https://www.cnn.com/2019/07/25/asia/internet-undersea-cables-intl-hnk/index.html.

The first issue concerning submarine internet cables concerns the way that the United States government uses these cables for surveillance purposes. Understanding the extent of the government's collection and usage of information collected is incredibly difficult for several reasons.[47] Due to the nature of surveillance programs as part of the national security apparatus, there is a large incentive to keep them private.[48] The hope being that by not disclosing the methods, agencies will be able to continue to use these programs without fearing that the targets will escape their notice.[49] To that effect, the state secrets doctrine has also protected large portions of the surveillance from being made public.[50]

With that all being said, some information about how the United States collects and use internet data has been disseminated.[51] Specifically, the National Security Agency, in its Upstream program, gets internet information by "compelling the assistance of telecommunications-services providers," on information that goes through the internet backbone.[52] . The NSA identifies the target of the surveillance, and sets the parameters for which the telecommunications-services providers must give the selected information to the government.[53]

---

[47] The government has not made this information public, and thus makes it very difficult to understand exactly what they are doing.
[48] *See* Wikimedia Foundation v. NSA/Central Sec. Serv., 857 F.3d 193, 202 (4th Cir. 2017) (saying that the United States government has acknowledged that internet surveillance programs exist, but that the methods are still classified).
[49] The United States has not explicitly stated why they have not declassified the information related to internet surveillance, but this supposition is based upon a logical conclusion based upon the facts available.
[50] U.S. v. Reynolds, 345, U.S. 1, 10 (1953); *See also* Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276, 294 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.) (holding that the state secrets privilege applies to foreign surveillance, and that it was proper to not allow discovery and dismiss the case).
[51] Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276, 280-81 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.) (providing a description of how the NSA conducts basic internet surveillance and its limitations).
[52] *Id.* at 280. The internet backbone consists of the internet cables, service stations, and submarine cables. *Id.*
[53] *Id.* at 280; Wikimedia Foundation v. NSA/Central Sec. Serv., 857 F.3d 193, 202 (4th Cir. 2017) ("The NSA performs Upstream surveillance by first identifying a target and then identifying 'selectors' for that target. Selectors are the specific means by which the target communicates, such as e-mail addresses or telephone numbers. Selectors cannot be keywords (e.g., 'bomb') or names of targeted individuals (e.g., 'Bin Laden')").

Upstream does not directly collect internet communications, but rather the information sent along the internet backbone.[54] Information sent along the internet backbone is not sent in discrete packages with just the specific information requested.[55] Instead, information sent along the internet backbone is transmitted by breaking the information down into packets.[56] Those packets can and do take a variety of different routes to the same destination.[57] In this process, the data packets will intermingle with other data packets in transit to form a complete internet transaction.[58] If information that is requested by the NSA is included with other data packets in that transaction, then the NSA will obtain all of the transaction and not just the requested information.[59]

This means that the NSA could potentially capture regular usage data from individuals who are not the target of the surveillance.[60] The NSA attempts to limit the capture of unintended data by emplacing a two-part filtering process.[61] The first filter attempts to eliminate any transactions which are domestic.[62] The second filter attempts to filter out any transactions which do not contain the specified parameters of the search information.[63] It is an open question as to whether these filters work to minimize data capture by the government.[64]

---

[54] Wikimedia Foundation v. NSA/Central Sec. Serv., 857 F.3d 193, 202-03 (4th Cir. 2017)
[55] *Id.* at 202-03.
[56] *Id.* at 203.
[57] *Id.* ("When an individual sends an email on the Internet, the message is broken up into one or more 'data packets' which are transmitted across the Internet backbone to their destination and, upon arrival, reassembled by the recipient's computer to reconstruct the communication.").
[58] Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276, 280 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.)

[59] *Id.*
[60] *Id.* at 280-81 (essentially the argument that the Wikimedia Foundation and other plaintiffs argue is happening).
[61] Wikimedia Foundation v. NSA/Central Sec. Serv., 857 F.3d 193, 203 (4th Cir. 2017).
[62] *Id.*
[63] *Id.* at 202-203 (this could be anything like the specified email address or phone number).
[64] Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276, 280-81 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.) (Wikimedia arguing that the NSA's program effectively captures nearly every Internet communication).

B. Private Use

Apart from the concerns of government surveillance, a large portion of the modern economy runs on personal information gleaned from the internet.[65] Based upon the fact that the United States government relies upon help from internet backbone operators to help obtain the information transmitted through their pipelines,[66] it is not impossible[67] If submarine cable operators do not currently engage in this specific behavior, it is still concerning that it could happen under the regulatory structure in place now.

Even if submarine cable operators do not directly collect and use information, plenty of other companies and other private entities track behavior on the internet.[68] This allows companies to effectively advertise to users of the internet.[69] As a consequence, the advertising technology space is forecasted to eclipse $1 trillion (about $3,100 per person in the US) in revenue by 2030.[70] There have been attempts to limit how much information companies can obtain from individuals in Europe[71] and in California.[72] With those large exceptions, people living in the United States are, by and large, uncovered by privacy protections.

III. How the Submarine Internet Cables Work and Operate

In order to understand why current regulatory structure exists, understanding how submarine telecommunications cables operate is key. Submarine internet cables and the internet

[65] Thematic Intelligence, *supra* note 6.
[66] Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276, 280 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.)

[67] There is no direct evidence of whether submarine cable operators collect and analyze personal information that transits through their pipelines, but nonetheless should be a concerning possibility that it could happen. The incentive to monetize every facet of a business is strong.
[68] Thematic Intelligence, *supra* note 6.
[69] Thematic Intelligence, *supra* note 6.
[70] Thematic Intelligence, *supra* note 6.
[71] Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation (GDPR).
[72] Cal. Civ. Code §§ 1798.100-1798.199.100 (CCPA amended by CPRA ballot initiative).

developed hand in hand.[73] Submarine cables physically connected countries across the seas at that offered a compelling combination of cost, ease of deployment, and information throughput.[74] The main alternative method of connecting the world is through satellites, but this ran into problems of cost.[75] Submarine cables in the 1980s carried vastly more data, at a faster speed, and for a cheaper cost than the alternative satellite communications systems.[76] Over time, cables have developed to carry more data for a "sufficiently low cost" to "allow the internet to grow."[77] However, satellite systems remain used today for the information transmission, but they do not form the backbone of international communication.[78] Whether the advent of new technology might change this calculus is still up for debate.[79] For instance, a modern fiberoptic cable allows "23 million simultaneous voice calls or around 1.9 million simultaneous transfers of 1Mb files."[80] As of 2020, there are a total of 475 submarine cables deployed all over the world connecting nations to one another.[81]

Submarine internet cables work by transmitting pulses of light through transparent fiber-optic cables over long distances to act as communications.[82] What this means is that information is transmitted by pulsing light.[83] It can be analogized to something like how a computer can read zeros and ones as information that can be quickly turned into a readable format. Underpinning any computer interface is a series of zeros and ones that form the basis of any information that

---

[73] BARTLETT-MCNEILL., *supra* note 2, at 15.
[74] *Id.*
[75] *Id.* at 16.
[76] *Id.*
[77] *Id.*
[78] *Id.*
[79] *See* Starlink, *Technology*¸ STARLINK (Oct. 23, 2022, 12:26 PM), https://www.starlink.com/technology.
[80] Lionel Carter and Douglas R. Burnett, *Chapter 23: Subsea Telecommunications*, IN ROUTLEDGE HANDBOOK OF OCEAN RESOURCES AND MANAGEMENT, 351 (2018).
[81] Justin Sherman, *Cyber Defense Across the Ocean Floor: The Geopolitics of Submarine Cable Security*, Atlantic Council, 6 (2021).
[82] LONNIE HAGADORN., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD, 18-19 (2009).
[83] *Id.*

you see on the screen. In a similar way, the light pulses of fiber optic cables send that information back and forth at incredible speeds.[84] So anytime someone needs to connect to a server or other computer across an ocean, they will be using submarine internet cables to carry that information. Any piece of data is split up and sent across one or more of the submarine cables when the server is outside of the United States.[85]

These cables are actually quite a bit smaller than one might expect. Cables laid in the deeper parts of the ocean have a diameter of a "garden hose (17-20 mm diameter)" and the more costal variants tend be a little larger at about "50 mm [in] diameter."[86] This relatively small size makes them comparatively easy to install on the ocean floor.[87] Partly due to this ease of installation, and partly due to the increased data capabilities of fiber-optics, this became one of the main mechanisms for connecting the world's internet.[88]

The other competitor for communications purposes was (and is) satellite communications.[89] However, this technology has significantly higher cost than the submarine fiber-optic cables.[90] It was estimated in 2007 that if every submarine internet cable was cut, "only 7% of the total United States traffic volume could be carried by satellite."[91]

A. Submarine Cables Operation in Practice

[84] Carter and Burnett, *supra* note 80, at 351.
[85] Wikimedia Foundation v. NSA/Central Sec. Serv., 857 F.3d 193, 203 (4th Cir. 2017) ("When an individual sends an email on the Internet, the message is broken up into one or more 'data packets' which are transmitted across the Internet backbone to their destination and, upon arrival, reassembled by the recipient's computer to reconstruct the communication.").
[86] HAGADORN, *supra* note 82, at 19.
[87] *Id.* (Coaxial cables required "four or five voyages" in order to lay a cable across the Atlantic, but fiber-optic cables reduced this down to only "one or two.").
[88] BARTLETT-MCNEILL., *supra* note 2, at 16.
[89] *Id.*
[90] *Id.*; *But see* Starlink, *supra* note 79.
[91] DOUGLAS R. BURNETT & LIONEL CARTER, INTERNATIONAL SUBMARINE CABLES AND BIODIVERSITY OF AREAS BEYOND NATIONAL JURISDICTION: THE CLOUT BENEATH THE SEA, Brill Res. Persp., L. Sea, 4 (2017).

For something that is so integral to the global economy and our daily lives, it seems outlandish that the government would allow private individuals to control the flow of information across continents. Contrary to what one might expect, the internet sea cable backbone from the United States is owned by private corporations.[92] This stands somewhat in contrast to other parts of the world where nation states own and operate their own international internet cable networks.[93] This means that the internet cables are not owned by the United States government, but rather private corporations.[94] Subject to certain limitations, the owners of submarine internet cables can use the cables as they see fit.[95]

However, that does not mean that these submarine cables are completely unregulated. In the United States, the Federal Communications Commission (FCC) regulates submarine cables, while the United Nation has promulgated the United Nations Convention on the Law of the Sea (UNCLOS) which provides international rules regarding submarine cables.[96]

However, these rules have proven to be inadequate for protecting both economic interests and consumers. There are two dueling issues pertaining to internet sea cables. The first is that the United States government appears able to directly tap into these cables and intercept all internet communications that occur on them with impunity.[97] A second, and related issue, there is a regulatory blind-spot to the same type of behavior by the corporations which own and operate sea cables. There does not seem to be any indication that these cable companies do engage in this

---

[92] Henry Goldberg, *One-Hundred and Twenty Years of International Communications*, 37 Fed. Comm. L.J. 131, 132 (1985).
[93] *Id.*
[94] *Id.*
[95] *See* Cable Landing License Act of 1921, ch. 12, 42 Stat. 8 (1921) (codified as amended 47 U.S.C. §§ 34-39); United Nations Convention on the Law of the Sea, art. 87, Oct. 12, 1982, 1833 U.N.T.S. 3 (UNCLOS); Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation (GDPR).
[96] Exec. Order No. 10530, 19 Fed. Reg. 2709 (May 10, 1954); United Nations Convention on the Law of the Sea (UNCLOS), Oct. 12, 1982, 1833 U.N.T.S. 3
[97] Case C-311/18, *Data Prot. Comm'n v. Facebook Ir. Ltd.* ("Schrems II"), ECLI:EU:C:2020:559 ¶¶ 62-65(Jul. 17, 2020); Khazan, *supra* note 3.

behavior, but there is very little to stop them from doing so. As privacy regulations in California[98] and other states start to make it more difficult to track online behavior, it might behoove a submarine cable owner to access information going through its cable to then sell. In addition, submarine cable operators have increasingly used internet connected remote management systems to control and monitor the cables.[99] This certainly gives great capability for submarine cable operators to monetize their connections that might not be immediately obvious to consumers.

IV. History of Internet Sea Cables in the United States

Submarine cables are older than one might expect, as a result the history of sea cables in the United States is a complicated one. As technology has changed and advanced, the laws have had to develop in conjunction with them. The first sea cables consisted of undersea copper cables that transmitted telegraphy signals across the Atlantic, starting in the 1850s.[100] These first cables simply carried electric beeps which formed the basis of international communication using telegraphs.[101] The first submarine cable was laid down in the English Channel "from Dover to Calais," during 1850.[102] The first submarine cable laid across the Atlantic Ocean did not happen until 1858 when a cable was laid between Newfoundland and Ireland.[103] Over time, the amount of information transmitted and the durability of the cables increased to make them a more form of international communications.[104]

The history of submarine cable regulations comes in three distinct historical segments. In the first period, during the technology's infancy, the President exercised their foreign affairs

[98] Cal. Civ. Code § 1798.100
[99] Sherman, *supra* note 81.
[100] HAGADORN, *supra* note 82, at 17.
[101] *Id.*
[102] BARTLETT-MCNEILL., *supra* note 2, at 11-12.
[103] *Id.* at 13.
[104] *Id.*

power to determine which submarine cables could land. After this approach was struck down by the courts in 1921,[105] Congress responded by passing the Cable Landing License Act of 1921.[106]This leads to the second period after Congress granted the President the authority to regulate submarine cable landings in the United States. The third period occurred during the deregulatory fervor after the 1970s. The third period leads to today with relatively little requirements for submarine cable operators.

A. Early Regulatory History of Submarine Cables (1800s-1921)

The first regulatory mechanisms were primarily based upon the President's foreign affairs powers.[107] The idea was that the President was acting in a diplomatic role that interacted with other foreign powers to land submarine cables. Companies would typically have a complete circuit from one foreign country to the United States.[108] In order for a foreign company to connect their cable to the United States, they would have to seek approval through the President.[109] This system worked on principles of "reciprocity", where the President would give approval to foreign cable connections to the United States if those same foreign nations would agree to allow connections to their country by United State companies.[110] This system of reciprocity did not last forever.

B. Regulatory History after *U.S. v. Western Union Telegraph Company* (1921-1970s)

The system of reciprocity ended when the Western Union Telegraph Company challenged whether the President had the authority to allow submarine cable landings without a statutory basis and to stop individuals from landing cables under the President's foreign powers

[105] United States v. W. Union Tel. Co., 272 F. 311, 321, 323 (S.D.N.Y. 1921).
[106] Cable Landing License Act of 1921, ch. 12, 42 Stat. 8 (1921) (codified as amended 47 U.S.C. §§ 34-39).
[107] Goldberg, *supra* note 91, at 133.
[108] *Id.*
[109] *Id.*
[110] *Id.*

authority..[111]Western Union responded to an action taken by the US to foreclose it from connecting a telegraph cable without the consent of the President.[112] Western Union presented a defense which resulted in the invalidation of the President's ability to approve cable landings based upon their foreign affairs powers.[113] As a consequence of this ruling by the Southern District of New York, "Congress enacted the Cable Landing License Act of 1921."[114] As the ability for the President to grant or deny the licenses for landing for these submarine cables had been negated, Congress needed to solve this issue. If Congress had not done so companies would have been able to land cables without any sort of regulatory approval. It also would have upset the system of reciprocity that drove the ability for American companies to land their cables on foreign shores.

The Cable Landing License Act of 1921 set up a period where AT&T dominated with submarine cables.[115] The President delegated the authority to grant landing licenses to the Federal Communication Commission (FCC).[116] "From 1927 to 1984, AT&T ha[d] been the sole entity providing telephone service from the United States to overseas points."[117] However, that is no longer the case, there are many cable owners besides AT&T.[118] There were other telegraph holders during this period, as opposed to telephone service.[119] Telegraphs are distinct from

[111] United States. v. W. Union Tel. Co., 272 F. 311, 321, 323 (S.D.N.Y. 1921).
[112] *Id.*
[113] *Id.* (Invalidating the ability of the President to deny landing licenses based upon the Interstate Commerce Act of 1866 and Supreme Court precedent); Goldberg, *supra* note 91, at 133.
[114] Goldberg, *supra* note 91, at 133; Cable Landing License Act of 1921, ch. 12, 42 Stat. 8 (1921) (codified as amended 47 U.S.C. §§ 34-39).
[115] Goldberg, *supra* note 91, at 134.
[116] Exec. Order No. 10530, 19 Fed. Reg. 2709 (May 10, 1954).
[117] Goldberg, *supra* note 91, at 134.
[118] TeleGeography, *Submarine Cable Map*, Submarine Cable Map (Oct. 23, 2022, 2:57PM) https://www.submarinecablemap.com.
[119] Goldberg, *supra* note 91, at 137.

telephones in the type of information that they transmit. Telegraphs allowed the communication of information by transmitting electric signals to be written on a piece of paper.[120]

However, when AT&T developed the technology to allow for both voice and telegraph information at the same time (coaxial), this made it so that the telegraph and telephone corporations were in competition.[121] The Communications Act was designed to regulate this nascent industry during the Great Depression era.[122] The act set the basis for how telecommunications companies would be regulated and set up their regulator in the form of the FCC.[123] For the most part, the FCC maintained a status quo of just a few cable operators to land in the United States by allocating the market and not allowing new entrants.[124]

C. Technological Advancements that Led to Today

The efforts of the FCC to maintain a status quo could not last forever. Technology advanced by the 1950s to include coaxial cables which increased the transmission capability of cable owners.[125] The first coaxial cable allowed for "about 36 individual voice channels."[126] In the next ten to twenty years, the amount of information that could be transmitted over these cables increased dramatically.[127] By this time, they could transmit "5,000 telephone calls," concurrently, though this increase in capacity also relied upon increase costs in signal boosters.[128] These coaxial cables were extraordinarily expensive to install across the ocean floor, as the size of the cables and the amount of repeaters required to ensure signal integrity were

[120] BARTLETT-MCNEILL., *supra* note 2, at 11.
[121] Goldberg, *supra* note 91, at 138-39.
[122] *Id.* at 134; Communications Act of 1934, ch. 652, 48 stat. 1064 (codified as amended 47 U.S.C. ch. 5).
[123] 47 U.S.C. § 154.
[124] Goldberg, *supra* note 91, at 134 ("committed the FCC to the role of cartel manager for a period of roughly thirty-five years thereafter").
[125] HAGADORN, *supra* note 82, at 18.
[126] *Id.*
[127] *Id.*
[128] *Id.*

commensurate with the amount of information that they carried.[129] High capacity coaxial cables could only be feasibly installed in the highest communications corridors as it was not cost effective in any other areas.[130]

Glass fiber-optic cables offered a solution to the ever increasing cost of information transmission.[131] Even the crudest fiber-optic cable far outstripped coaxial's ability to transmit information.[132] The information transmission capacity of fiber-optic cables has only increased over time, as current cables allow for "over 1 million telephone calls."[133] In 1988, the first fiber-optic (glass) cable was laid in the Atlantic.[134] This is the current technology used for submarine cables that carry information.[135] The technology has not remained static, with improvements in the design of the glass fibers which has allowed for specialization in the cable design depending upon the use case.[136] The relative cheapness of this technology has allowed the internet to expand greatly since the first submarine internet cable was laid down in 1988.[137] The vast majority of international communications use submarine internet cables to transmit information.[138]

D. Deregulatory Efforts in Submarine Cables (1980s-Today)

---

[129] *Id.* (Signal repeaters would have to be placed every "6-9 km in the highest capacity systems.").
[130] BARTLETT-MCNEILL., *supra* note 2, at 15 ("[T]he bulk of global trans-oceanic traffic [was] carried by satellites," as a consequence of the high cost involved with installing coaxial cables).
[131] *Id.*
[132] *Id.* ("Glass fibres could carry 12,000 channels, compared to 5,500 for the most advanced coaxial cable.).
[133] HAGADORN, *supra* note 82, at 19 (2009)
[134] *Id.* at 18; BARTLETT-MCNEILL., *supra* note 2, at 15-16 (The first submarine test of the fiber-optic test occurred in 1979, and successfully proved that these cables could withstand the rigors of duty underwater. The first international fiber-optic cable deployment occurred in the relatively short crossing between the United Kingdom and Belgium in 1986.).
[135] HAGADORN, *supra* note 82, at 19 (2009) (The exact design of the fiber-optic cables has changed over time, but the fundamental principles behind their use remain the same. For instance, the type of signal repeaters and the amount of impurities found within the glass fibers have changed over time.).
[136] *Id.*
[137] BARTLETT-MCNEILL., *supra* note 2, at 16.
[138] BURNETT & CARTER, *supra* note 90 at 3.

During the second period of the FCC's life as a regulator, it acted to maintain a careful balance between the few telecommunications corporations that operated submarine cables by trying to maintain a status quo.[139] The FCC could effectively control who entered the telecommunications industry through the regulatory approval process.[140] By the late 1970s and into the 1980s, the deregulation infatuation started to take hold.[141] Changes in FCC rules allowed new cable operators to land in the United States so long as they "obtain[ed] operating agreement with foreign carriers prior to the initiation of service."[142] The FCC was still relying upon the Cable Landing License Act of 1921 as the basis for their regulatory choices, but they chose to take a different tack from the previous administrations.

This resulted in the FCC allowing new entrants into the international telecommunications industry so long as they could get foreign landings for their cables.[143] Functionally, the regulatory landscape for submarine communications cables has come "full circle."[144] The FCC now generally allows for new entrants into the submarine cable industry, rather than maintaining nascent cartels as it did during the early to mid-1900s.[145] At that time, there was a change in philosophy on how best to grow the telecommunications industry.[146] The change in policy made it much easier for new entrants to come into the marketplace.[147] The entry of new submarine cable operators generally is allowed under the FCC's rules.[148] The rules for new entrants to the

[139] Goldberg, *supra* note 91, at 146.
[140] *Id.* at 147-48.
[141] *Id.* at 147.
[142] *Id.*
[143] *Id.*
[144] *Id.* at 152 (remarking that the regulatory choices for which cable landings to allow is much more free flowing now than it was during much of the 20th century).
[145] Goldberg, *supra* note 91, at 152-53.
[146] *Id.*
[147] *Id.*
[148] *Id.* at 147.

submarine cable industry are not simple, but they generally allow companies to land in the United States so long as they fulfil the requirements set out by the FCC.[149]

The flexibility for the regulatory system governing submarine internet cables suggests that the system could be changed again to suit a different purpose. This flexibility would theoretically allow the President and FCC to make changes to better information privacy protections. The history of FCC's regulatory ability suggest that change is possible.

E. Effects on Global Economy

International submarine internet cables play a crucial role in the global economy. Many of the global banking institutions rely heavily upon the internet access provided by submarine internet cables to connect them to other countries in near real time.[150] On a daily basis, these cables provide trillions of dollars a day in processing.[151] It's not just banking that relies upon the interconnections provided by submarine internet cables.[152] Pretty much any company which interacts with the global economy such as "shipping companies, airlines, banks, supply chain, manufacturing businesses, and entertainment[,] would be crippled without access to international markets.[153]

V. Regulation of Internet Submarine Cables in the United States

In the modern day, regulation of internet submarine cables in the United States is mostly the purview of the FCC.[154] The FCC determines whether a submarine cable will have authorization to land in the United States.[155] Each submarine cable that would like to connect to

[149] *Id.*
[150] BURNETT & CARTER, *supra* note 90 at 4.
[151] *Id.*
[152] *Id.* at 5.
[153] *Id.*
[154] Exec. Order No. 10530, 19 Fed. Reg. 2709 (May 10, 1954).
[155] *Id.*

the United States must fill out an application to the FCC in accordance with their regulations.[156] The application must include items such as the "list of proposed owners", where the cable will land in the United States, a description of the cable; whether the cable will be operated as a common carrier, and other important questions.[157]

A. FCC and Basic Regulations of Submarine Cables

Once a cable operator has been granted license to land in the United States, it still falls within the purview of the FCC to regulate the continued existence of the license.[158] Nevertheless, the FCC may revoke a landing license for a number of reasons, including: promoting security, "maintaining the rights or interests of the United States," "assur[ing] just and reasonable rates and service," or to help gain landings/operations in foreign countries.[159]

The FCC's ability to regulate submarine cables stems from the President's authority to grant or revoke landing licenses under the Cable Landing License Act of 1921, which was created through a challenge of the President's inherent foreign affairs powers.[160] The President has since transferred this regulatory regime to the FCC.[161] The FCC's purview already covered related areas of law concerning telecommunications, and the President delegated the authority to regulate submarine cables through executive order.[162] Under the regulatory power of the FCC, a company must satisfy several conditions in order to be granted a license,[163] with one of the most important conditions being whether a cable operator comes under the purview of the FCC as a

[156] 47 C.F.R. §1.767 (2022).
[157] *Id.*
[158] Exec. Order No. 10530, 19 Fed. Reg. 2709 (May 10, 1954).
[159] *Id.;* 47 U.S.C. § 35.
[160] Cable Landing License Act of 1921, ch. 12, 42 Stat. 8 (1921) (codified as amended 47 U.S.C. §§ 34-39); Henry Goldberg, *One-Hundred and Twenty Years of International Communications*, 37 FED. COMM. L.J. 131, 133 (1985).
[161] Exec. Order No. 10530, 19 Fed. Reg. 2709 (May 10, 1954).
[162] *Id.*
[163] 47 C.F.R. §§ 1.767 (2022).

common carrier or a non-common carrier.[164] When applying for a cable landing license, a cable operator has to make the determination for itself whether they will be operating as a common carrier.[165]

B. FCC's Determination of Common Carrier or Non-Common Carrier Status

Determining whether a cable licensee operates as a common carrier depends on whether the cable licensee fulfills the requirements set out in *National Association of Regulatory Utility Commissioners v. FCC*.[166] If the cable operator fulfills the requirements as a common carrier, then it would have to apply as a common carrier to the FCC.[167] Common carriers typically conduct activities in a "quasi-public character" where "the carrier 'undertakes to carry for all people indifferently. . . .'"[168] When something is identified as a common carrier, this has been "used to impose a greater standard of care upon carriers who held themselves out as offering to serve the public in general."[169] Common carriers have a "stricter duty of care" due to their "implicit[] accept[ance]. . .of public trust by availing themselves of the business of the public at large."[170]

The statute governing the FCC defines a "common carrier", as related to submarine internet cables, as "any person engaged as a common carrier for hire, in interstate or foreign communication by wire or radio."[171] A designation as a common carrier often meant that the

---

[164] 47 C.F.R. §§ 1.767(a)(6) (2022); FEDERAL COMMUNICATIONS COMMISSION, SUBMARINE CABLE LANDING LICENSES (BACKGROUND), https://www.fcc.gov/research-reports/guides/submarine-cable-landing-licenses (last visited Nov. 19, 2022).
[165] 47 C.F.R. §§ 1.767(a)(6) (2022).
[166] *Id.*; FEDERAL COMMUNICATIONS COMMISSION, SUBMARINE CABLE LANDING LICENSES (BACKGROUND), https://www.fcc.gov/research-reports/guides/submarine-cable-landing-licenses (last visited Nov. 19, 2022); Nat'l Ass'n of Regul. Util. Comm'rs v. FCC, 525 F.2d 630, 642 (D.C. Cir. 1976).
[167] 47 C.F.R. §§ 1.767(a)(6) (2022).
[168] Nat'l Ass'n of Regul. Util. Comm'rs v. FCC, 525 F.2d 630, 641 (D.C. Cir. 1976) (quoting Semon v. Royal Indem. Co., 279 F.2d 737, 739 (5th Cir. 1960).
[169] Nat'l Ass'n of Regul. Util. Comm'rs, 525 F.2d at 640.
[170] *Id.* at 641.
[171] 47 U.S.C. § 153 (11).

carrier would face more stringent requirements for their operation.[172] Under Title II of the Communications Act, common carriers must provide "nondiscriminatory access to network elements," as well as requiring "just and reasonable," communication service that includes "charges, practices, classifications, and regulations".[173] Under *National Association of Regulatory Utility Commissioners v. FCC*, which the FCC uses to determine eligibility for non-common carrier status, the key question is whether the "operator offer[s] indiscriminate service to whatever public its service may legally and practically be of use." If the submarine cable operator determines that it will operate as a common carrier, it must then "obtain a separate carrier license (in addition to the cable landing license). ."[174]

In the home internet market, the FCC made the broad determination that cable companies that provided internet service did not come under the purview of regulations related to common carriers.[175] The home internet market is comprised of services such as cable internet and fiber internet operators but does not include submarine cable operators.[176] When considering whether to apply common carrier status to cable company internet service providers, the FCC ruled that the "cable companies do not ' offe[r] telecommunications service to the end user, but rather... merely us[e] telecommunications to provide end users with cable modem service.'"[177] This limited the applicability of the greater regulatory power that the FCC has over common

---

[172] Nat'l Ass'n of Regul. Util. Comm'rs 525 F.2d at 641.
[173] 47 U.S.C. § 201; *see* Rob Frieden, *The Rise of Quasi-Common Carriers and Conduit Convergence*, 9 A J. OF L. & POL'Y 471, 473 n.1 (2015) (discussing the various duties attached when something is identified as a common carrier under Title II of the Communications Act).
[174] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, 10 (2016) (citing 47 U.S.C. § 214; 47 C.F.R. § 1767(g)(4)).
[175] Frieden, *supra* note 173, at 477; In re Inquiry Concerning High-Speed Access to Internet Over Cable and Other Facilities, 17 FCC Rcd. 4798, 4801-02 (2002) (aff'd by Nat. Cable & Tele. Ass'n v. Brand X Internet Serv., 545 U.S. 967, 979 (2005)).
[176] *See* Frieden, *supra* note 179; In re Inquiry Concerning High-Speed Access to Internet Over Cable and Other Facilities, 17 FCC Rcd. 4798, 4801-02 (2002) (aff'd by Nat. Cable & Tele. Ass'n v. Brand X Internet Serv., 545 U.S. 967, 979 (2005))
[177] Nat. Cable & Tele. Ass'n v. Brand X Internet Serv., 545 U.S. 967, 979 (2005) (quoting In re Inquiry Concerning High-Speed Access to Internet Over Cable and Other Facilities, 17 FCC Rcd. 4798 (2002)).

carriers.[178] However, this determination ~~about cable companies~~ does not appear to have ~~that this has~~ affected the determination of whether submarine cable providers come under the purview of regulation as common carriers.[179] There are an equal number of both common carrier and non-common carrier applications to the FCC for submarine cable landing licenses or renewals.[180]

As of the November 20, 2022, there are six total pending new cable landing licenses or renewal applications.[181] Three of the six pending cable landing licenses are for common carrier status, and three with non-common carrier status.[182] Furthermore, the FCC has generally allowed "agreements for the exchange of Internet traffic," to be "unregulated and left solely to commercial negotiation between Internet backbone providers."[183] These types of peering agreements typically involve either a like-kind exchange of access (where similar traffic patterns exist) or a paid access to the network.[184] Ultimately, the ability to label submarine cables as common carriers could grant the FCC greater power to regulate the submarine cables if the FCC changes how it defines common carriers to include more submarine cables.

C. FCC Regulation on Transfer and Reporting Submarine Cable Licenses

Through authority provided by executive order and the Cable Landing License Act, for a number of years, the FCC required that cable operators give the FCC yearly reports on the amount of revenue gained from the submarine cable, the amount of traffic, and reports on the

[178] *See also id.*
[179] *See* FEDERAL COMMUNICATIONS COMMISSION, PENDING SUBMARINE CABLE APPLICATIONS, https://www.fcc.gov/pending-submarine-cable-applications (last visited Nov. 20, 2022).
[180] *Id.*
[181] *Id.*
[182] *Id.*
[183] Daniel L. Brenner & Winston Maxwell, *The Network Neutrality and the Netflix Dispute: Upcoming Challenges for Content Providers in Europe and the United States*, 23 INTELL. PROP. & TEHC. L.J. 3, 5 (2011).
[184] *Id.*

status of submarine cable circuits.[185] The FCC changed the reporting requirements in 2017, and under the new rules, cable owners and operators are not obligated to report their revenue or traffic.[186]

Now, stakeholders of cable landing licenses only need to file a yearly report to the FCC on the capacity of their cable.[187] In the last report on the number of "FCC licensed submarine cable systems," the FCC listed 83 as "either operating or planning to enter service," in May of 2022.[188] This gives the FCC less information to work with in order to make determinations about the best way to regulate the use of submarine cables. In addition, cable operators cannot "transfer[], assign[], or dispose[] of. . .control of the licensee," without the consent of the FCC.[189] If a submarine cable operator wishes to make changes to their submarine cable landing license, they must seek approval from the FCC.[190]

D. National Security Concerns in Submarine Cable Regulation

When a submarine cable has any foreign investment or lending, these arrangements will be scrutinized under a separate national security review that is not directly part of the FCC.[191] The FCC has the authority to refer the cable landing licenses to other Executive Branch agencies when considering issues of national security under Team Telecom.[192] Team Telecom includes

---

[185] 47 C.F.R. § 43.62 (no longer in effect); FEDERAL COMMUNICATIONS COMMISSION, IN THE MATTER OF REPORTING REQUIREMENTS FOR U.S. PROVIDERS OF INTERNATIONAL TELECOMMUNICATIONS SERVICES, 579-80 (2013).
[186] FEDERAL COMMUNICATIONS COMMISSION, CIRCUIT CAPACITY DATA FOR U.S.-INTERNATIONAL SUBMARINE CABLES, https://www.fcc.gov/international/circuit-capacity-data-us-international-submarine-cables (last visited Nov. 19, 2022); 47 C.F.R. § 43.82.
[187] 47 C.F.R. § 43.82.
[188] FEDERAL COMMUNICATIONS COMMISSION, SUBMARINE CABLE LANDING LICENSES (LICENSED CABLES), https://www.fcc.gov/research-reports/guides/submarine-cable-landing-licenses (last visited Nov. 19, 2022).
[189] 47 C.F.R. § 1.767(g)(6).
[190] *Id.*
[191] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, 11 (2016); RULES AND POLICIES ON FOREIGN PARTICIPATION IN THE U.S. TELECOMMUNICATIONS MARKET, REPORT AND ORDER AND ORDER ON RECONSIDERATION, 12 FCC Rcd. 23891, ¶¶ 61-66 (1997).
[192] *Id.*

"Departments of Defense, Homeland Security, and Justice (including the Federal Bureau of Investigation). "[193] Team Telecom only conducts reviews of new cable landing licenses applications when "(1) the system will connect the United States to a foreign point, or (2) the system will have aggregate direct or indirect foreign ownership of 10 percent or more."[194]

The actions of Team Telecom are not "pursuant to any law," and Team telecom "has not promulgated any regulations governing its substantive requirements and procedures."[195] Nonetheless, Team Telecom acts fairly consistently in performing their reviews.[196] It is the official policy of the FCC to defer "to the Executive Branch on issues of national security, law enforcement, and public safety[.]"[197] Unless Team Telecom grants their approval, the FCC will not grant a landing license.[198] The Team Telecom review takes a significant amount of time and is the largest source of delay when the FCC is considering granting a cable license.[199]

Under the current system, the U.S. Department of State (with consultation of U.S. Departments of Defense and Commerce) has the "final review and approval" of a cable landing license.[200] This review by the Department of State is completely separate from the Team Telecom review for national security purposes.[201] This is the final review process in the submarine cable landing license process.[202]

E. State Submarine Cable Regulation

---

[193] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191 at 11-12.
[194] *Id.* at 12.
[195] *Id.*
[196] *Id.*
[197]FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 12;
[198] *Foreign Participation Order*, 12 FCC Rcd. at 23, 919-20 ¶ 63.
[199]FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 12.
[200] *Id.* at 10; Exec. Order No. 10530 § 5, 19 Fed. Reg. 2709 (May 10, 1954).
[201] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 10.
[202] *Id.*

Due to the federal system of government in the U.S., states do have some ability to affect how submarine cables land within their jurisdiction.[203] Under the Coastal Zone Management Act of 1972 [204], the coastal states which have "coastal zone management plans, under which the states and territories regulate activities within or affecting a state or territory's sea," may act upon a "right to review permitting and licensing activities by federal government agencies."[205] States have an outer seaward boundary of three "geographical miles distant from its coast line or, in the case of the Great Lakes, to the international boundary."[206] As of 2016, no state or territory had "ever requested such a consistency review of an FCC cable landing license application," but that does not mean that one will never occur.[207] While this is one way that the states could work to effectuate change in the way that the FCC governs submarine cable landings, it does not guarantee that a change will occur.

F. Environmental Regulations Concerning Cable Landing

After granting approval for a landing license, the regulatory approvals do not end with that for submarine cable operators.[208] For instance, a submarine cable might have to gain approval for the U.S. Army Corps of Engineers for affecting the navigable waters of the United States.[209] When the submarine cable operators lay down their cables, they might have to interact with other agencies with jurisdiction over areas such as natural resources such as natural gas.[210] When the cable is actually near landing at a specific state or territory, the submarine cable

[203] Coastal Zone Management Act of 1972 (codified as 16 U.S.C. §§ 1451-64).
[204] *Id.*
[205] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 11.
[206] 43 U.S.C. § 1312.
[207] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 11.
[208] *Id.* at 12-13.
[209] *Id.*
[210] *Id.* at 20.

operator would have to gain approval from these local authorities on issues related to environmental impact and landing approval.[211]

VI. Regulatory History of Submarine Cables in the International Context

The United States must also contend with international law and treaties when considering how to handle submarine cables. By their very nature, submarine cables traverse international waters and must connect with other nations to be effective. ~~as the connections between nations.~~ The "first ever 'law of the sea' treaty" involved the protection of submarine cables.[212] The Paris Convention for the Protection of Submarine Telegraph Cables in 1884 ~~(Paris Cable Convention)~~ resulted in the first agreement to the effective neutrality of the cables outside the boundaries of the territorial waters of the agreeing countries.[213] Generally speaking, the Paris Cable Convention is now "accepted as customary international law."[214] As a result, the rules contained within the Paris Cable Convention are still used to this day.[215] Furthermore, the Paris Cable Convention served as the precursor and foundation to later international agreements on submarine cables.[216]

The Paris Cable Convention is not the only governing authority for submarine cables. In the realm of international law, the ability to lay and repair submarine cables is governed by the United Nations Convention on the Law of the Sea (UNCLOS).[217] The rights and duties of states who have signed UNCLOS are fairly simple. In the "exclusive economic zone," only the country

---

[211] *Id.* at 32.
[212] BURNETT & CARTER, *supra* note 90 at 7 (suggesting that the 1884 International Convention for the Protection of Submarine Cables was the first international law of the sea treaty).
[213] Convention for the Protection of Submarine Telegraph Cables, Paris (Mar. 14, 1884) (Available through NOAA: https://www.noaa.gov/gc-international-section/submarine-cables-international-framework).
[214] Restatement (Third) of Foreign Relations Law § 521 comt. F (Am L. Inst. 1987).
[215] DOUGLAS BURNETT, SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD, INTERNATIONAL LAW, 26 (2009).
[216] Lionel Carter & Douglas R. Burnett, *Subsea Telecommunications*, ROUTLEDGE HANDBOOK OF OCEAN RESOURCES AND MANAGEMENT, 351 (2018).
[217] United Nations Convention on the Law of the Sea, Oct. 12, 1982, 1833 U.N.T.S. 3.

with that exclusive economic zone has the right to lay submarine cables within that area.[218] The "exclusive economic zone," is defined as not "extend[ing] beyond 200 nautical miles from baselines."[219] The baseline is simply the "low-water line along the coast."[220] On the "continental shelf," "[a]ll states" have the rights to "lay submarine cable."[221]

UNCLOS defines the "continental shelf," as going "beyond its territorial sea," up to the "continental margin" or up to "200 nautical miles," if the continent does not extend up to that distance. [222]Similarly, in the high seas, all states have the "freedom to lay submarine cables."[223] The definition of the high seas encompasses all parts of the seas which are not "included in the exclusive economic zone, in the territorial sea or in the internal waters of a State, or in the archipelagic waters of an archipelago State."[224]

The United States never officially ratified the UNCLOS as required under the Constitution.[225] While this treaty has never been ratified, the United states has traditionally followed the basic agreements found within the agreement.[226] President Ronald Reagan published a proclamation that established that the United States had an exclusive economic zone which encompassed a "distance 200 nautical miles from the baseline."[227] This proclamation specifically laid out that the United States would not infringe upon the rights of other nations to lay "submarine cables," on the high seas.[228] President William J. Clinton published a

---

[218] United Nations Convention on the Law of the Sea, art. 50, Oct. 12, 1982, 1833 U.N.T.S. 3.
[219] *Id.* art. 57 (noting that the exact measurement of the baseline can change depending upon the exact topography of the country in question).
[220] *Id.* art. 55.
[221] *Id.* art. 79.
[222] *Id.* art. 76.
[223] *Id.* art. 87.
[224] *Id.* art. 86.
[225] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 4 n. 10 (Noting that the United States did sign UNCLOS, but it was never ratified as required, by the United States Senate).
[226] Delimitation of the Maritime Boundary in the Gulf of Maine Area (Can. V. U.S.), 1984 I.C.J Rep. 246, 294 ¶94 (1984).
[227] Proclamation No. 5030, 48 Fed. Reg. 10,605 (Mar. 10, 1983).
[228] *Id.*

proclamation that established the United States as having a "contiguous zone" that "extends to 24 nautical miles from the baselines of the United States."[229]

In the international community the United States is treated as if it follows customary international law regardless of whether the United States signed UNCLOS .[230] The International Court of Justice argued in effect ~~that the fact~~ that the United States had already declared its intent to follow one provision (the exclusive economic zone), and that the President had noted that the "Convention generally confirmed existed rules of international law."[231] As a consequence, even though UNCLOS had not yet come into effect at the time of the judgment, the United States is treated as if it follows customary international law.[232] This sets the some of the limits of the United States' jurisdiction over submarine cables.[233] There have been some other treaties and agreements which form the basis of the limitations and rights related to laying cables.[234]

The history of submarine telecommunications cables and their regulation in the United States has not had a linear trajectory, despite the fact that internet cables represent the vast majority of international communications traffic.[235] The regulation of internet submarine cables abroad? follows a similarly snaking path. The relative scarcity of international requirements means that cable operators do not have to comport themselves to any behaviors.

VII. Regulation of Internet Sea Cables in the International Community

[229] Proclamation No. 7219, 64 Fed. Reg. 48,701 (Aug. 2, 1999).
[230] Delimitation of the Maritime Boundary in the Gulf of Maine Area (Can. V. U.S.), 1984 I.C.J Rep. 246, 294 ¶94 (1984).
[231] *Id.*(it should be noted that this decision occurred before President William J. Clinton reinforced the United States compliance with the strictures of UNCLOS).
[232] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 4 n.10; Delimitation of the Maritime Boundary in the Gulf of Maine Area (Can. V. U.S.), 1984 I.C.J Rep. 246, 294 ¶94 (1984).
[233] FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191, at 3.
[234] Convention for the Protection of Submarine Telegraph Cables, Mar. 14, 1884, 24 Stat. 989, 25 Stat. 1424.*see also* FCC CSRIC FINAL REPORT–INTERAGENCY AND INTERJURISDICTIONAL COORDINATION, *supra* note 191 at 3 fn. 2).
[235] MICK GREEN ET AL., SUBMARINE CABLES AND THE OCEANS: CONNECTING THE WORLD, 3 (2009).

In the modern day, the international regulatory system of submarine internet cables is somewhat less complicated than that of the United States. Fundamentally, each nation state has their own regulatory requirements for what needs to be done in order to land a submarine cable, but how the international community interacts with each other's cables is governed by treaty.[236] The Paris Cable Convention is still used today as a detailed framework for how to implement the submarine cable standards of UNCLOS.[237] However, the Paris Cable Convention is still only applicable today for the 36 nations (United States included) who signed the agreement.[238] In the international context, both UNCLOS and the Paris Convention provide the backstop for how nations will interact with each other over the issue of laying and maintaining submarine communications cables.

A. International Framework for Laying and Maintaining Submarine Cables

The Paris Cable Convention sets out some basic rights and duties for signing nations related to submarine telegraph cables.[239] This agreement only applies to submarine cables "outside territorial waters."[240] The protections under this agreement provide that it is "a punishable offense to break or injure a submarine cable,"; that a party breaking a cable would have to bear the cost of that breakage; and that any ship which has to sacrifice their equipment to ensure the survival of a submarine cable would be indemnified.[241] In addition, the home country

[236] United Nations Convention on the Law of the Sea, art. 87, Oct. 12, 1982, 1833 U.N.T.S. 3 (UNCLOS)
[237] Carter & Burnett, *supra* note 217, at 351 n.1.
[238] Nat'l Oceanic and Atmospheric Admin., *Submarine Cables – International Framework*, (Mar. 1, 2019), https://www.noaa.gov/gc-international-section/submarine-cables-international-framework.
[239] Convention for the Protection of Submarine Telegraph Cables, Paris (Mar. 14, 1884) (available through NOAA: https://www.noaa.gov/gc-international-section/submarine-cables-international-framework).
[240] *Id.*
[241] *Id.* art. IV, VII.

of the vessel that breaks the submarine cable has the responsibility to punish the offending parties under the Paris Cable Convention.[242]

The application of this treaty has been sporadic.[243] There have been very few publicly available instances where a vessel would actually face action based upon their destruction of cables.[244] One of the only applications of the Paris Convention treaty occurred in 1959 between a United States naval ship and a Soviet Union trawler.[245] In this instance, a U.S. naval ship boarded the Soviet fishing boat after a series of five submarine telecommunication cable breaks.[246]

UNCLOS provides more applicable regulations to submarine cables in the international context. Under the auspices of UNCLOS, there are "the freedoms to lay, maintain and repair cables outside of territorial seas."[247] In the same vein, nation states with coastal waters and other pipeline and cable owners must "not take actions that prejudice the repair and maintenance of existing cables."[248] UNCLOS also highlights additional requirements such as requirements for submarine cable maintenance as well as protective measures for cable related accidents.[249] Functionally, the rights and duties under UNCLOS are fairly simple for the signatory nations.

---

[242] *Id.* art. VIII; U.S. DEP'T OF STATE, DEP'T OF STATE BULLETIN, VOL. XL, NO. 1034, 557 (1959) (available at: https://www.noaa.gov/gc-international-section/submarine-cables-international-framework).
[243] *See* Nat'l Oceanic and Atmospheric Admin., *Submarine Cables – International Framework*, (Mar. 1, 2019), https://www.noaa.gov/gc-international-section/submarine-cables-international-framework.
[244] *Id.*
[245] *Id.*; U.S. DEP'T OF STATE, DEP'T OF STATE BULLETIN, VOL. XL, NO. 1034, 555-58 (1959) (available at: https://www.noaa.gov/gc-international-section/submarine-cables-international-framework).
[246] *Id.* at 555.
[247] Carter & Burnett, *supra* note 217, at 352; United Nations Convention on the Law of the Sea, art. 112, Oct. 12, 1982, 1833 U.N.T.S. 3.
[248] Carter & Burnett, *supra* note 217, at 352; United Nations Convention on the Law of the Sea, art. 79, Oct. 12, 1982, 1833 U.N.T.S. 3.
[249] Carter & Burnett, *supra* note 217, at 352 (noting the requirement that boats that snag a cable on their anchors or fishing line must let loose those lines, and that the cable owners must indemnify those who let loose their lines, noting that domestic laws apply to those who purposefully or negligently cut cables, and mentioning that states with coastline and other cable/pipeline owners must not take prejudicial action on the maintenance and repair of existing cables); United Nations Convention on the Law of the Sea, art. 113-15, Oct. 12, 1982, 1833 U.N.T.S. 3.

These signatory nations have control over submarine cables within their ocean territory and there is a general right to lay cables in parts of the ocean not claimed by other nations.[250] In addition, signatories must not prejudice those cables which have already been laid.[251]

Within the "continental shelf," coastal nation states have the right to lay submarine cables and set standards and conditions upon which submarine cables can connect to their lands.[252] This allows individual nation states to ~~still~~ establish their own requirements for allowing cable landings in their country as the United States has done.[253] The specific cable regulations ~~will~~ vary by country, but the regulations allow nation states ~~will~~ each ~~have the ability~~ to control what cables ~~who~~ will be able to land in their country. ~~and continue to be landed within the country.~~

B. Effect of GDPR on Submarine Cable Owners

In addition to international agreements, information privacy laws also ~~are not the only laws which could~~ potentially apply to submarine cable owners. ~~On the issue of information privacy~~ The EU regulates the types of behaviors that entities may engage in when dealing with citizens of the EU or when the entity is physically located in a EU country.[254] The purpose of the General Data Protection Regulation (GDPR) in the EU is to "protect[] fundamental rights and freedoms of natural persons and in particular their right of the protection of personal data."[255] To that effect, it limits the data that entities can collect from covered individuals.[256]

In the context of information privacy, it is likely that the submarine cable operators fall within the auspices of the GDPR for the purposes of covered individuals.[257] The GDPR covers

[250] United Nations Convention on the Law of the Sea, art. 113-15, Oct. 12, 1982, 1833 U.N.T.S. 3
[251] United Nations Convention on the Law of the Sea, art. 79 (5), Oct. 12, 1982, 1833 U.N.T.S. 3
[252] United Nations Convention on the Law of the Sea, art. 79, Oct. 12, 1982, 1833 U.N.T.S. 3.
[253] *Id.*
[254] Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation (GDPR). art. 4.
[255] *Id.* art. 1 (2) (Setting out the objectives and purposes of the GDPR).
[256] *Id.* at art. 5.
[257] *Id.* at art. 3.

entities that act as "controllers" and "processors" which are not mutually exclusive.[258] Processing means "any operation or set of operations. . . performed on personal data or on sets of personal data."[259] Controller simply means the entity which decides how or whether the personal data collected will be processed.[260] The personal data covered by this regulation include "any information relating to an identified or identifiable natural person."[261]

In the event that submarine cable operators collect any data that passes through their pipeline, they would most likely be defined as controllers. ~~Submarine cable operators would most likely fit under the definition of controllers they collect any of the data.~~ At the same time, if they then decided to analyze or disseminate the personal data in any way, then they may additionally be defined as a ~~this would probably also fit the definition of a~~ processor. As a result in the case that submarine cable operators collected information from their pipelines, many ~~submarine cable~~ operators would likely fit the description of a covered entity. ~~The~~ Covered entities encompass ~~cover~~ broad swaths of companies that interact with data in disparate ~~some~~ forms. ~~or another.~~ If the submarine cable operators are considered ~~potentially~~ covered entities, then the question becomes whether they fall within the scope of the GDPR.

The scope of the GDPR not only includes companies and individuals within the European Union, but also ~~privacy rights associated with the GDPR cover~~ controllers or processors physically located in the EU.[262] In addition, the GDPR covers controllers and processers outside the EU when they offer goods or services to individuals within the EU, or they monitor the behavior of the covered EU individuals.[263]

---

[258] *Id.* at art. 4.
[259] *Id.* at art. 4 (2).
[260] *Id.* at art. 4 (7).
[261] *Id.* at art. 4 (1).
[262] *Id.* at art. 3 (1).
[263] *Id.* at art. 3 (2).

In the case that submarine cable operators engage in the data collection, it is likely that any cable connected to Europe (or the United Kingdom)[264] would fall under the scope of the GDPR.[265] Due to the fact that the landing locations for submarine cables to the European Union have to be physically located in the European Union, these cable operators would most likely fall within the scope of the GDPR.[266] It is hard to imagine a cable that connects physically with countries covered by the GDPR would not fall within this definition, but the submarine cables that do not connect to the EU might not fall within the scope of the GDPR.[267] It is unlikely that submarine cable operators would offer goods or services to EU individuals. However, it is possible that submarine cable operators, if they do track EU individuals, would come under the auspices of the GDPR.

VIII. Solutions

There is no one solution to the issues concerning information privacy and submarine cables. What would work for the issue with regard to government surveillance would probably not work for private surveillance. As a result, there needs to be individualized solutions to the problems of surveillance. Government capture of information is particularly troublesome, as there are no easy solutions. In contrast, surveillance by private entities might have a relatively simple solution.

A. Government Use

[264] Data Protection Act of 2018, c. 12 (U.K) (United Kingdom implemented their own version of the GDPR that is still in effect even after the United Kingdom left the European Union).
[265] Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation, art. 4 (GDPR).
[266] *See id.* art. 4.
[267] *See id.*

The government uses submarine internet cables for covert surveillance for national security threats.[268] Government surveillance of submarine internet cables does not have a simple solution. There are basically two different options. The first option comes down to the President setting out an Executive Order ordering the various national security agencies to not engage in this type of surveillance. The other option would be to go through Congress to pass a law to restrict the ability for the government to spy on people through submarine cables. As this is an issue of national security, the courts tend to give great deference to the President on this issue.[269]

There are some limits to what types of surveillance that the Executive Branch can engage in,[270] but those limits for activities associated with foreign powers and their agents are limited.[271] When considering any type of surveillance by the United States, the Constitution, the Wiretap Act, and the Foreign Intelligence Surveillance Act (FISA) provide the limits of the government's ability to surveil individuals.[272]

The Constitution, and specifically the Fourth Amendment, protects against surveillance by the government on domestic security threats and regular criminal investigations.[273] The Supreme Court has not specifically said whether the Fourth Amendment applies to surveillance

---

[268] *See* Wikimedia Found. v. NSA/Central Sec. Serv., 857 F.3d 193, 202 (4th Cir. 2017) (stating that the United States government has acknowledged that internet surveillance programs exist, but that the methods are still classified).
[269] Wikimedia Found. v. NSA/Central Sec. Serv., 14 F.4th 276, 294 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.) (holding that the state secrets privilege applies to foreign surveillance, and that it was proper to not allow discovery and dismiss the case).
[270] United States v. United States Dist. Court for Eastern Dist. of Mich., So. Div., 407 U.S. 297, 317-18 (1972) (holding that cases of surveillance of internal domestic security issues requires some form of prior approval from a magistrate on "whether there is probable cause for surveillance" but does not specifically determine whether the Fourth Amendment applies to surveillance of activities of foreign powers and their agents) (referred to hereinafter as The Judge Keith Case); and Katz v. United States, 389 U.S. 347, 353, 355-6 (holding that the 4th Amendment requires judicial authorization by warrant on probable cause of the crime committed and that it must comply with the Wiretap Act.).
[271] 50 U.S.C. §§ 1802, 1804, 1881.
[272] *Id.*
[273] The Judge Kieth Case, 407 U.S. at 317-18 (1972); Katz 389 U.S. at 353, 355-6.

of foreign powers and their agents.[274] Instead, Congress passed the Foreign Intelligence Surveillance Act (FISA) to limit the federal government's ability to conduct foreign surveillance.[275]

i. The Constitution and Regular Criminal Case

The government cannot just engage in spying upon people in the United States without their permission or a court order.[276] The Wiretap Act sets the warrant standard for intercepting "wire, oral, or electronic communication," for the purpose of ordinary crime.[277] If the United States would like to intercept the communications of an individual within the United States for ordinary crimes, the Fourth Amendment and the Wiretap procedures will apply.[278]

ii. The Constitution and Domestic National Security Threats

In addition to not being able to spy on individuals within the United States involved in regular criminal activity without a court order, the United States cannot engage in private information collecting for domestic individuals accused of engaging in activities that threaten national security. The Judge Keith Case lays the limits for what the United States can do in obtaining information about individuals in a private situation.[279]

---

[274] The Judge Kieth Case, 407 U.S. at 308-09 (1972).
[275] S. Rep. No. 95-701, at 6 (1978) (suggesting the purpose of the FISA Act of 1978 was to "provide a statutory procedure to authorize applications for a court order approving the use of electronic surveillance within the United States to obtain foreign intelligence information").
[276] *Katz*,389 U.S. at 353, 359 (holding that recording of an individual without a warrant as insufficient for the purposes of the 4th Amendment) (" The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment."); 18 U.S.C. § 2511; U.S. v. Jones, 565 U.S. 400, 404 (2012) (holding that the "installation of a GPS devise on a target's vehicle, and its use of that device to monitor the vehicle's movements, constitutes a 'search.'") (suggesting that the Fourth Amendment primarily protects against trespasses on property and not when individuals have a reasonable expectation of privacy as in *Katz*); Carpenter v. U.S., 138 S.Ct. 2206, 2217 (holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements," as captured by cellphone tracking of location through a wireless carrier and that it constitutes a search under the Fourth Amendment).
[277] 18 U.S.C. §§ 2516-18 (commonly referred to as the Wiretap Act).
[278] *Katz*,= 389 U.S. at353, 359; 18 U.S.C. §§ 2516-18.
[279] The Judge Keith Case, 407 U.S. at 317-18 (1972)

iii. Standing and the State Secrets Doctrine

Even if a party wants to a challenge government surveillance, there are two major problems with applying a challenge toward government capture and use of private information from the Internet. The first issue is whether the plaintiff alleging an injury has the standing to sue the federal government under Article III of the Constitution.[280] In the second problem, the States Secrets Doctrine acts as a privilege for the government to keep from disclosing information when it might implicate a negative impact on the interests of national security.[281]

Under the current application of the standing requirement "an injury must be 'concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling.'"[282] In the context of government surveillance, a "speculative chain of possibilities," does not support a finding of standing.[283] This seems to suggest that simply the possibility of being the subject of surveillance without the knowledge of the surveillance does not form a sufficient basis for standing.[284]

On the other hand, the State Secrets Doctrine requires that courts accept a claim of privilege by the government in limited circumstances.[285] The Supreme Court has said that when "there is a reasonable danger that compulsion of the evidence will expose military matters which, in the interest of national security, should not be divulged," the court should allow the application of privilege in that situation.[286] This extends to even prohibiting the judge from viewing the evidence in their chambers alone.[287]

---

[280] Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013).
[281] U.S. v. Reynolds, 345 U.S. 1, 10 (1953); Wikimedia Foundation v. NSA/Central Sec. Serv., 14 F.4th 276, 282 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.).
[282] *Clapper*,568 U.S. at 409 (quoting Monsanto Co. v. Geertson Seed Farms, 561, U.S. 139 (2010)).
[283] *Id.* at 414.
[284] *Id.* at 414-16.
[285] *Reynolds*, 345 U.S. at10 (1953).
[286] *Id.*
[287] *Id.*

iv. Surveillance of Foreign Threats Capturing Non-Threats

Since the Supreme Court has never answered the question as to whether the Fourth Amendment covers foreign surveillance, Congress enacted FISA to provide some procedures for engaging in this type of surveillance.[288] Section 1881a of FISA creates the procedures for surveillance of individuals located outside of the United States who are not United States citizens.[289] In order to ensure that compliance with the requirements of the law, "FISA created two specialized courts—the Foreign Intelligence Surveillance Court (the "FISC"), from which the government generally must obtain authorization before conducting electronic surveillance, and the Foreign Intelligence Surveillance Court of Review, which has jurisdiction to review the denial of a FISA application for electronic surveillance."[290]

The design of Section 1881a specifically avoids "particularity and probable cause requirements in . . . surveillance [which] allows the government to monitor the communications of thousands of individuals and groups under a single FISC Order."[291] Even when the government complies with minimization procedures, the government can still retain the information of U.S. persons if "the government concludes that they contain 'foreign intelligence,' information."[292]

Section 1881a clearly does not provide enough privacy protections for individuals. Unfortunately, the State Secrets Doctrine and Standing requirements make it exceedingly

[288] S. Rep. No. 95-701, at 6 (1978).
[289] 50 U.S.C. § 1881a(a) ("[T]he Attorney General and the Director of National Intelligence may authorize jointly, for a period of up to 1 year from the effective date of the authorization, the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information.")
[290] Wikimedia Foundation v. NSA/Central Sec. Serv., 857 F.3d 193, 200 (4th Cir. 2017)
[291] *Id.* at 201.
[292] *Id.*

difficult to challenge the application of foreign surveillance through the court system.[293] With inaccessibility to the court system on this issue, the only real solution would be for either Congress or the President to change the procedures required to surveil foreign individuals. One potential solution could be to require that agencies have probable cause to surveil individuals which would avoid some of the issues where thousands of individuals could be caught in one FISC order. Ultimately, Congress or the President could act to ameliorate the risks of non-related information being caught by foreign intelligence gathering missions by enacting changes to these programs through executive order or legislation.

v. The Way Forward

Ultimately, this means that any attempts to changing government surveillance faces significant challenges. It is clear that the Constitution is not sufficient to protect information privacy rights in all circumstances.[294] As a consequence, the only realistic options would be to go through executive action or through Congressional action. The best solution would be to sign into law a comprehensive set of privacy rights such as those granted by the GDPR,[295] or to a lesser extent the CPRA.[296] By giving individuals protections in how their data is used, this could help ameliorate some of the issues involved with government surveillance and capture of data through submarine cables.

This theoretical law could place strictures on how the government may capture and use data, while also giving greater oversight to how that data is used. This law would need to contain some form of oversight to ameliorate issues with the State's Secrets doctrine. Without oversight

[293] Wikimedia Foundation v. NSA/Central Sec. Serv., 14 F.4th 276, 294 (4th Cir. 2021), *cert denied* 2023 WL 2123742 (mem.) (holding that the state secrets privilege applies to foreign surveillance, and that it was proper to not allow discovery and dismiss the case).
[294]The Judge Keith Case , 407 U.S. 297, 308-09 (1972).
[295] Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation.
[296] Cal. Civ. Code §§ 1798.100-1798.199.100 (CCPA amended by CPRA ballot initiative).

mechanisms, it's possible that any privacy rights granted could be effectively unenforceable. Of course, the likelihood of passing any piece of legislation is staggeringly small. If legislation cannot be passed, the best hope would be to petition the President to minimize the damage done by this kind of surveillance.

B. Private Use

While government use of private information through submarine cables does not have an easy or simple solution, the potential use of private information by private submarine cable holders might.. With the potential for use of submarine internet cables as a vehicle for gaining private information, there is a need for a solution. The unique way that the United States regulates the laying and maintenance of submarine cables offers a unique opportunity to affect the way that private entities from obtaining and using personal data. The Cable Landing License Act of 1921 offers the President broad discretion on whether to grant or withhold cable landing licenses.[297] In fact, the relevant portion of the revised Cable Landing License Act of 1921 provides that:

> The President may withhold or revoke such license when he shall be satisfied after due notice and hearing that such action will assist in securing rights for the landing or operation of cables in foreign countries, or in maintaining the rights or interests of the United States or of its citizens in foreign countries, or will promote the security of the United States, or may grant such license upon such terms as shall be necessary to assure just and reasonable rates and service in the operation and use of cables so licensed.[298]

The broad, and discretionary language, in the Cable Landing License Act gives the President a lot of flexibility in how to regulate submarine cable operators.

[297] Cable Landing License Act of 1921, ch. 12, 42 Stat. 8 (1921) (codified as amended 47 U.S.C. §§ 34-39).
[298] 47 U.S.C. § 35.

The President could potentially order that submarine cable operators could not collect any individual information from their cables. Under the *Youngstown* framework, it is quite possible that the President would be able to regulate the submarine cable industry quite effectively through executive action.[299] Due to the express delegation by Congress to authorize and revoke cable landing licenses, the President's power is at its peak.[300]

i. The Non-Delegation Doctrine and Submarine Cables

Under the Non-Delegation Doctrine, Congress cannot delegate its power to the President to make laws.[301] However, the last time that the Supreme Court invalidated a law for violating the non-delegation doctrine was in 1935.[302] However, this does not mean that this doctrine is completely dead. Instead, it has taken a more indirect form. Courts will narrowly construe a statute to ensure that it conforms with the non-delegation doctrine rather than completely invalidate a law.[303]

The GDPR offers one way to limit some of the ability of submarine cable operators to use their cables to invade personal privacy.[304] However, the scope of the GDPR is limited to certain circumstances which might not effect many Americans.[305] While the GDPR might look like a

[299] Youngstown Sheet & Tube Co. v. Sawyer, 343 U.S. 579, 585-86 (1952) ("The President's power, if any, to issue the order must stem either from an act of Congress or from the Constitution itself."); *Id.* at635-38 (Justice Jackson's Concurrence) (suggesting that the President's authority to take action is at its greatest when acting "pursuant to an express or implied authorization of Congress" as this power basically "includes all that he possesses in his own right plus all that Congress can delegate.").
[300] *Id.*
[301] A.L.A. Schecter Poultry Co. v. United States, 295 U.S. 495, 529-30 (1935).
[302] Kathryn A. Watts, *Rulemaking as Legislating*, 103 GEO. L. J. 1003, 1012 (2017).
[303] Margaret H. Lemos, *The Other Delegate: Judicially Administered Statutes and the Nondelegation Doctrine*, 81 S. CAL. L. REV. 405, 455-56 (suggesting that courts will narrowly construe a statute when there is too much of a delegated authority to be constitutionally viable, but still allowing the statute to be in effect in a limited capacity).
[304] Commission Regulation 2016/679 of May 25, 2018, General Data Protection Regulation (GDPR).
[305] *Id.* at art. 3(1-2) (Controllers who have an establishment in the European Union and controllers and processors outside the EU where processing of personal data is related to offering goods or services to data subjects in the EU or the monitoring of EU data subjects behavior).

great solution, it only really solves the issue of companies using private information for those under the auspices of the GDPR, which does not affect many Americans.[306]

ii. Freedom of Speech Conflicting with Privacy

One concern might be whether the freedom of speech to commercialize information might conflict with efforts to effectuate privacy related policies.[307] The First Amendment requires that "Congress shall make no law...abridging the freedom of speech, or of the press; or the right of the people to peaceably to assemble, and to petition the Government for a redress of grievances." [308] The "creation and dissemination of information are speech within the meaning of the First Amendment." [309]

In *Sorrell*, Court has said that "it is the State's burden to justify its content-based law as consistent with the First Amendment."[310] Any attempts by the President to use their power to grant cable landing licenses might run afoul of the requirements in *Sorrell*.[311] It's unknown whether the application of the Cable Landing License Act of 1921 would violate the First Amendment if it was used to limit the acquisition of individual's private data, but it is possible that the government could pass this burden.[312] Even should a challenge on free speech grounds arise, it would still be worthwhile to attempt to ensure the privacy rights of all individuals

iii. The Way Forward

---

[306] *Id.*
[307] Sorrell v. IMS Health Inc., 564 U.S. 552, 571-72 (2011).
[308] U.S. CONST. amend. I.
[309] *Sorrell*,564 U.S. at571-72.
[310] *Id.*
[311] *Id.* at 557 (holding that a law that "restricts the sale, disclosure, and use of pharmacy records that reveal the prescribing practices of individual doctors," as violating the First Amendment). *But see id.* at 567 ("It is true that restrictions on protected expression are distinct from restrictions on economic activity or, more generally, on nonexpressive conduct.").
[312] The exact analysis would depend upon how the Executive Branch designed the restrictions on submarine cable operators, but if the restrictions are based upon all collection and sale of individual information, it would probably not come under the definition of content or speaker based restrictions of speech. *See Sorrell*, 564 U.S. at564.

Even with all of the potential challenges, using executive action to stop or prevent the potentially problematic capture of private information by private entities could be a valid method for protecting information privacy rights. Of course, a comprehensive law which sets out specific privacy rights would be preferable, but that might be difficult to accomplish due to the nature of politics in the United States. Therefore, using executive action with a basis in the Cable Landing License Act of 1921 is a viable alternative. An executive action would not necessarily have to be particularly complicated. It could set out that any future use of submarine cables to collect personal data would be the basis for a rescission of a cable landing license in the United States.

Taking this to its logical extreme, the President could attempt greater regulation on the telecommunications industry writ large through the Cable Landing License Act of 1921. Logically, if an end user internet provider would like to provide internet access to the countries outside of the United States, it must sign agreements with a submarine cable operator or more than one. It seems possible that the President could set a requirement that every submarine cable operator connected to the United States would be required to only allow connections with other cable operators which do not collect personal data. This means that the President could potentially act to enforce greater privacy rights for individuals by leveraging the cable landing licenses that submarine cable operators rely upon. Internet providers must connect to locations throughout the world, and limiting the access of internet providers to submarine cables in the United States could be a way to effectively guard information privacy rights. If submarine cable operators would lose their landing license for doing business with an internet service provider that collects personal data, this could effectively limit this behavior. Ultimately, the Cable Landing License Act of 1921 offers many opportunities to effect change related to submarine cables.

If the President cannot or will not use the Cable Landing License Act of 1921 as the basis for executive action, then there are other options. The most significant would be to rely upon the FCC and its ability to regulate common carriers.[313] Some submarine cable operators already come under this definition[314], but the FCC could attempt apply common carrier status to other submarine cable operators. The FCC regulations allow the commission "to impose common carrier regulation or other regulation consistent with the Cable Landing License Act on the operations of the cable systems if it finds that he public interest so requires[.]"[315] This could potentially offer an alternative to using executive action. Assigning all submarine cable operators as common carriers would give the FCC greater ability to regulate the cable operators' behaviors. For instance, there are certain privacy protections to telecommunications information that flows across common carrier lines.[316]

IX. Conclusion

The regulatory structure built around the use of submarine cables provides both opportunity and danger for the privacy of individuals in the United States. There are two main dangers associated with the current regulatory structure of the submarine cables. The first is government surveillance, with the second being surveillance by entities other than governments. As the law is currently applied, individuals can be surveilled by the government and by private entities.

While the law, as applied right now, might create issues for information privacy, there is some opportunity to fix these issues. The Cable Landing License Act of 1921 gives the President

[313] 47 C.F.R. §§ 1.767(a)(6).
[314] FCC, *supra* note 178.
[315] 47 C.F.R. § 1767(g)(10).
[316] 47 U.S.C. § 222. *But see* 47 U.S.C. § 222 (d) (allowing common carriers to use and disclose "customer proprietary network information" that covers a broad range of information that could still be useful to advertisers and data-miners).

the power to enact significant change on the information privacy landscape. Even if the President cannot or will not act on private surveillance by submarine internet cables, the FCC could still act by changing how it characterizes submarine cable operators. By characterizing submarine cable operators as common carriers, it would give the FCC greater regulatory power over them. At the same time, there is a blind spot in how the government acquires and analyzes foreign intelligence under the auspices of national security. With the seeming incapability of change through the court system, the only option is to seek change through the executive or legislative branch. Congress and the President could enact comprehensive privacy rights for individuals that would curtail the worse of the abuses possible in the current situation.