Quantum Bits of Light: The Future of Quantum Key Distribution under Export Administration Regulations and the First Amendment

*Marshall Mckellar**

1. Introduction

Over two thousand years ago, Julius Caesar maintained military secrecy by using a process already ancient in its application. Trusting no one (including his messengers), Ceasar replaced every A in his messages with a D, every B with an E, and so on for every letter in the alphabet, ensuring that only someone who knew the "shift by 3 key" could decipher his messages. This process of using a secret "key" to correctly assemble a jumbled, unintelligible mess of letters is called encryption.[1] Two millennia later, the military strategists of Nazi Germany implemented a similar (yet dramatically more sophisticated) encryption method using their famed Enigma machines. Only after years of endless labor by many of the world's most talented cryptographers—along with significant advances in computing technology—was the Enigma code cracked, allowing Allied forces to gain an upper hand in the Atlantic theatre.[2]

Modern advances in encryption technology such as the quantum key distribution method—using entangled photons to transmit secret keys[3]—have begun a worldwide race to achieve truly unbreakable cryptography. In a world held captive by constantly emerging stories of cyber-attacks, national security breaches, and government mass surveillance; issues involving privacy and communication technology are now at the forefront of cultural dialogue.

* University of Mississippi School of Law.

1 PGP Version 6.5.1: Introduction to Cryptography 1, *available at* http://openpgp.vie-privee.org/doc_en.html (last visited February 22, 2018). [hereafter, PGP Introduction].

2 Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998), *rev'd*, 209 F.3d 482 (6th Cir. 2000).

3 Eleni Diamanti, Hoi-Kwong lo, Bing Qi, and Zhiliang Yuan, *Practical Challenges in Quantum Key Distribution,* NPJ: QUANTUM INFORMATION 1 (Nov. 8, 2016).

Within the past several years, secure communication icons like Edward Snowden, Julian Assange, and Anonymous have become household names, greatly influencing international politics and mainstream media. The key ingredient to many of these world-changing events is reliable encryption methods, allowing information activists to securely and anonymously communicate anything from personal emails to top secret government files.

Due to its powerful social and military uses, encryption technology was closely regulated in the United States under the International Traffic in Arms Regulations (ITAR) for many years. However, this began to change in 1999 when President Clinton transferred commercial encryption technology from the ITAR to the Export Administration Regulations (EAR) regime.[4] Although this act had the appearance of reducing some regulatory hurdles for the export of encryption, the Government maintained a consistently firm grip on nearly every facet of encryption technology. Both before and after the Clinton shift, cryptographers brought suits against the government to enjoin the enforcement of any regulation whatsoever on 1990's era cryptography, claiming free speech protection as enshrined in the First Amendment of the United States Constitution. Two notable plaintiffs eventually won influential holdings from both the 6th[5] and 9th[6] federal circuit court of appeals.

Although issues related to encryption source code have been adjudicated in the federal court system with some positive results, the future of cryptography—specifically advances associated with quantum cryptography (quantum key distribution)—remains unsecured under both federal First Amendment jurisprudence and the EAR. This article will seek to illuminate the legal landscape surrounding encryption and suggest both judicial and regulatory clarifications to help ensure the future accessibility and use of quantum encryption technology. This article will first provide a brief overview of how modern commercial encryption works, describing how it has advanced in recent years from fairly straightforward computer software to ultra-sophisticated methods of transmitting secret keys using the physics of quantum entanglement.[7] Next, it will summarize key court decisions related to encryption and the first amendment; namely, Junger v. Daley and Bernstein v. Department of Justice. This article will then analyze the current regulatory framework for the export of quantum cryptography technologies under Category 5, Part 2 of the Export Administration Regulation's Commerce Control List. Finally, this article will assess—in light of current

4 Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1136 (9th Cir.), reh'g granted, opinion withdrawn, 192 F.3d 1308 (9th Cir. 1999). [Hereafter, Bernstein v. Dep't of Justice].

5 Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998), *rev'd*, 209 F.3d 481 (6th Cir. 2000).

6 Bernstein v. U.S. Dep't of Justice.

7 PGP Introduction; Sheng-Kai Liao, *et al, Satellite-to-Ground Quantum Key Distribution*, 549 NATURE (August 9, 2017).

EAR regulations and Junger/Daley—whether the future development and potential widespread public use of quantum cryptographic technology in the United States is at risk under the current judicial landscape/export regulatory regime, and what changes are necessary to protect it.

2. Encryption: A Brief Overview

2.1 Conventional and Public Key Cryptography

The primary purpose of cryptography is to ensure secrecy and confidentiality. In an alternate universe built entirely on trust, the science of cryptography would exist only as a mathematical game; however, in this reality, cryptography is the means by which two people may exchange information in such a way as to protect it from the prying eyes of untrusted third parties. Encryption serves as a powerful shield against totalitarian regimes, snooping government agencies, and even our favorite social media providers.

As previously mentioned, encryption has origins as a weapon of war, only recently becoming accessible to the American public during the Clinton Era.[8] However, even before the Clinton administration moved encryption technologies from the ITAR to the EAR, an anti-nuclear activist named Phil Zimmerman developed an encryption program called Pretty Good Privacy (PGP) and—in 1991—uploaded it to a primordial version of the internet.[9] PGP spread like wildfire across the globe, finding its way into democratic and totalitarian/communist countries alike.[10] Zimmerman's program became the archetype for how modern cryptography is used and understood by the masses. Using the relative simplicity of PGP as a helpful example, this section will provide a brief overview of how modern encryption works. It will then briefly assess one of the world's most anticipated encryption technologies—quantum key distribution (QKD)—and its potential world-shaping applications.

To better understand how encryption works, let's use our friends, Harry and Ginny, as an example. Harry writes Ginny an email in standard English professing his love for her; this standard email message is called *plaintext* or *cleartext*.[11] However, Harry has a nagging suspicion that Ginny's father, Severus, secretly has access to Ginny's school email account from his reconnaissance castle in Hungary . In order to ensure that only Ginny can read his epic love letter, Harry looks for free encryption software on the internet. Good encryption software would allow Harry to encrypt his plaintext letter, turning it into a heap of "unreadable gibberish" called

8 *Supra*, note 4.
9 ANDY GREENBERG, THIS MACHINE KILLS SECRETS 70-93 (2012).
10 *Id.*
11 PGP Introduction, at 1.

ciphertext.[12] Harry quickly finds several "conventional" encryption programs that use something called a *key*—essentially a gigantic numerical value that plugs into a cryptographic algorithm—to mathematically scramble (encrypt) and unscramble (decrypt) his plaintext letter.[13] However, this conventional encryption method has potential security risks. Because conventional cryptography uses a single key to both encrypt and decrypt a plaintext, Harry would need to communicate the secret key to Ginny so she could use it to decrypt and read Harry's email. This would be a non-issue if Ginny still lived in the apartment down the street from Harry's townhouse in Hogsmeade, but alas, she is on summer vacation in the Galapagos islands studying Hungarian Horntail dragons. Ginny's only method of communication is through her email account.

Fearing that Severus would intercept an email containing his secret key, Harry abandons conventional encryption in favor of a more secure alternative called *public key cryptography* (PKC). Unlike conventional encryption, PKC uses at least two keys for encryption: a public (non-secret) key for encrypting plaintext, and a corresponding secret key for decrypting it.[14] Instead of sending a shared secret key across potentially unsecure networks, Harry and Jill can each create a public key and share them freely online, whilst keeping their private keys safely hidden on a local hard-drive.[15] Harry would then encrypt his love letter using Ginny's easily accessible public key.[16] Because the numerical value of Ginny's secret key is derived directly from her public key, it ensures that Ginny alone can open an email encrypted by her public key. Although it is theoretically possible to extract Ginny's secret key from her public key, such a feat would require computing resources beyond that of her snooping father.[17] One of the most prolific, user friendly versions of public key cryptography is none other than a free version of Phil Zimmerman's PGP software called OpenPGP. OpenPGP is public key encryption with an additional (third) key to help protect a user's secret key from potential attackers.[18]

Because most encryption "hacking" techniques (a.k.a. cryptanalysis) use data patterns found within a plaintext to unscramble its cyphertext, OpenPGP first compresses the plaintext, reducing patterns in the plaintext data to greatly enhance its encryption strength.[19] Next, OpenPGP encrypts the compressed plaintext with a randomly generated, one-time *session key*. The program then encrypts that one-time session key using the intended

12 *Id.*
13 *Id.* at 2.
14 *Id.* at 4
15 *Id.*
16 *Id.*
17 *Id.*
18 *Id.*
19 *Id.*

recipient's public key. Finally, this two-fold encryption package is sent to the recipient, who can then use his/her secret key to unlock the public key encrypted one-time session key. This in turn can decrypt a ciphertext into readable plaintext.[20] Consequently, even if Severus intercepts Harry's email, he will receive nothing more than an infinitely complex jumble of meaningless characters. With no plaintext data patterns to crack and Ginny's secret key hidden safely in the Galapagos islands, Harry and Ginny's love story remains as it should: private.

Although Harry and Ginny's use of public key encryption may thwart Severus at first, their communications remain at risk. For example, Severus could download OpenPGP and create a private/public key pair that looks nearly identical to Ginny's, potentially fooling Harry into encrypting his communications to Severus' public key. To help battle potential identity fraud, OpenPGP implements an identity authentication system using *digital signatures* [21] and *hash functions*.[22] On its face, digital signatures are fairly simple: "instead of encrypting information using someone else's public key, you encrypt it with your private key. If the information can be decrypted with your public key, then it must have originated with you;" thereby assuring authenticity of origin.[23] Hash functions take a "variable length input—in this case, a message of any length, even thousands or millions of bits—and produces a fixed length output."[24] The final result is an encrypted digital signature that cannot be altered or detached from the document in any way without causing the digital signature verification process to fail.[25]

2.2 Quantum Key Distribution

Unfortunately, even if Harry and Ginny implement OpenPGP's three-key system and digital signature verification process, Severus could potentially—given enough time—invest all of his assets to build a supercomputer capable of extracting Ginny's secret key from her public key. This is the inherent problem for practically all encryption systems that rely on "the perceived computational intractability of certain mathematical functions."[26] Despite the mathematic complexity of public key algorithms, "such schemes do not provide information-theoretic security because they are vulnerable to future advances in hardware and algorithms."[27] One of the most radical threats to public key encryption methods is the development of powerful quantum

20 *Id.* at 5.
21 *Id.* at 6.
22 *Id.*
23 *Id.* at 5.
24 *Id.* at 6.
25 *Id.*
26 Sheng-Kai Liao, at 1.
27 Eleni Diamanti, Hoi-Kwong lo, Bing Qi, and Zhiliang Yuan, at 1.

computers.[28] Ironically, this purported bane of effective cryptography is also its potential savior. Whereas quantum computers will likely render obsolete the algorithmic firewalls of public key encryption, quantum encryption may soon redefine the science of cryptography by providing practically fail-proof secret key distribution.

Quantum cryptography promises "unconditional security—the Holy Grail of communication security—based on the laws of physics alone."[29] The principle behind QKD's effectiveness is the *quantum non-cloning principle*, which "forbids eavesdroppers from creating copies of a transmitted quantum cryptographic key."[30] To illustrate how QKD works, let's return to our hopeless lovers, Harry and Ginny. Much to their dismay, Severus sells his reconnaissance castle to purchase a brand new quantum supercomputer for the sole purpose of decrypting Harry and Ginny's secret keys from their public keys. In response, the ever resourceful couple hires their brilliant friend, Dobby, to build a sophisticated QKD system they can use to thwart Severus' newfound computing power. Current QKD systems are designed to transmit information by sending entangled pairs of single photons through either optical fibers (lines of fiber-optic cables), free space (satellite-to-ground transmission), or a combination of the two methods.[31] This allows distant users to securely produce a secret key made up of "a common, random string of secret bits," capable of encrypting and decrypting confidential messages.[32]Because mere observation alone disturbs particles at the quantum level, "any eavesdropper on the quantum channel attempting to gain information of the key will inevitably introduce disturbance to the system, and can be detected by the communicating users."[33] The benefits of such a system guarantee users not only the potential un-crackability of secret keys (for now), but also unquestionable certainty as to whether a secret key experienced any attempted observation or tampering. This technology would allow for an unprecedented level of confidence in secure-communication.

28 *Id.*

29 Eleni Diamanti, Hoi-Kwong lo, Bing Qi, and Zhiliang Yuan, at 1; Sheng-Kai Liao, at 1.

30 The no-cloning theorem, QUANTIKI (October 26, 2015). https://www.quantiki.org/wiki/no-cloning-theorem. (last visited April 16, 2018). "Fundamentally, the no-cloning theorem protects the uncertainty principle in quantum mechanics. If one could clone an *unknown* state, then one could make as many copies of it as one wished, and measure each dynamical variable with arbitrary precision, thereby bypassing the uncertainty principle. This is prevented by the non-cloning theorem."

31 Sheng-Kai Liao, at 1.

32 *Id.*

33 Sheng-Kai Liao, at 1; Duncan Graham-Rowe, Quantum Cryptography for the Masses, MIT TECHNOLOGY REVIEW (August 28, 2009). https://www.technologyreview.com/s/415073/quantum-cryptography-for-the-masses/. (Last visited April 16, 2018).

2.2.1 The Optical Fiber Method

The most straightforward method of practicing QKD is by sending photons through fiber optic cables. However, the effectiveness of this system decreases exponentially as distance increases. Unlike traditional forms of telecommunications, "the quantum signal in QKD cannot be noiselessly amplified due to the quantum non-cloning theorem. This limits the maximal distance for secure QKD to a few hundred kilometers."[34] In fact, a recent study by Chinese scientists calculated that sending even a single bit key over a 1,200 km fiber would take approximately six million years.[35] Despite this significant hurdle, companies around the world are developing technology to solve the problem of distance for key transmission across fiber. [36]

2.2.2 The Satellite-to-Ground Method

A more promising solution for efficient global QKD is through quantum satellites in space. Due to the relative thinness of the Earth's atmosphere in low-earth-orbit, "satellite-to-ground connections has significantly reduced losses. This is mainly because . . . most of the photon's propagation path is in empty space with negligible absorption and turbulence.[37] China is currently experimenting with satellite-based QKD using its Quantum Experiments at Space Scale (QUESS) spacecraft, the very first quantum satellite launched into orbit.[38] The QUESS spacecraft has successfully performed QKD during daily routines of 273 second periods, and at distances of up to 1200 kilometers.[39] During the course of these 273 second periods, ground stations collected as many as 1,671,072 bits of sifted keys.[40] To put this performance level in perspective, "at 1200 km, the satellite-based QKD within the 273 s coverage time demonstrates a channel efficiency that is ~20 orders of magnitudes higher than using the optical fiber."[41] In short, the future of cryptography is space-based.

---

34 Sheng-Kai Liao, at 1, 3.
35 *Id*. at 6.
36 Battelle to test quantum key distribution on Ohio fiber-optic network, Lightwave (September 8, 2014). http://www.lightwaveonline.com/articles/2014/09/battelle-to-test-quantum-key-distribution-on-ohio-fiber-optic-network.html. (Last visited April 16, 2018); Duncan Graham-Rowe;
37 Sheng-Kai Liao, at 2.
38 Mike Wall, "China Launches Pioneering 'Hack-Proof' Quantum-Communications Satellite," SPACE.COM (August 16, 2016), *available at*, https://www.space.com/33760-china-launches-quantum-communications-satellite.html. (last visited, March 14, 2018); Gabriel Popkin, "China's quantum satellite achieves 'spooky action' at record distance." SCIENCE (June 15, 2017), *available at*, http://www.sciencemag.org/news/2017/06/china-s-quantum-satellite-achxieves-spooky-action-record-distance. (last visited March 14, 2018).
39 Sheng-Kai Liao, at 6.
40 *Id*.
41 *Id*. at 7.

2.2.3 Future applications

If the future of effective private communication is dependent on immeasurably expensive trans-continental fiber-optic cables and billion-dollar quantum satellites, the general public is at a severe disadvantage compared to the deep pockets of mega-corporations and world governments. Thankfully, there has been a "tremendous scientific and engineering effort" towards creating a global quantum internet, complete with accessible QKD encryption.[42] By syncing a series of quantum satellites in a constellation around the Earth, quantum keys can be distributed from New York to Sydney with relative speed and efficiency.[43] Short fiber-optic cables could then be used to create metropolitan quantum networks, "sufficient and convenient co connect numerous users within a city at ~100 km scale."[44] Such networks would make quantum cryptography available on a global scale;

> The long term vision is for each user to use a simple and cheap transmitter and outsource all the complicated devices for network control and measurement to an untrusted network operator. The important advantage is that the network operator can be completely untrusted without compromising security.[45]

Although the demise of public key encryption is likely a ship fast approaching on the horizon, QKD must overcome a litany of challenges before it is ready to replace its conventional predecessor. Developers must launch many QKD-capable satellites at higher orbits, increase com-link efficiency, employ more advanced telescopes for tracking, and enhance wave-front correction capabilities before quantum satellite constellations become sufficiently reliable.[46] However, before this wondrous technology becomes widely accessible in the United States, it would behoove secure communication advocates to assess whether the current judicial and regulatory infrastructure is prepared to facilitate these advances in technology and privacy. If QKD is the future of secure communication, should it not be protected as zealously as communication itself?

3. Encryption and the Courts

Encryption as a scientific and communicative discipline has experienced relatively little adjudication in the United States. The Lion's share of judicial

42 Eleni Diamanti, Hoi-Kwong lo, Bing Qi, and Zhiliang Yuan, at 1.
43 *Id*. at 9.
44 *Id*.
45 *Id*. at 8.
46 Sheng-Kai Liao, at 9.

material is derived from two district court cases: Junger v. Daley[47] and Bernstein v. U.S. Dep't of Justice.[48] Despite both cases dealing almost exclusively with mere source-code for encryption software, the holdings from both the 6th and 9th circuit provide helpful insight as to how the judicial system will likely approach the use of encryption-related technologies going into the future. This section will analyze the holdings from both cases, with an eye towards how the Courts' decisions could potentially impact the future use and development of encryption technologies like QKD.

3.1 Bernstein v. U.S. Dep't of Justice

Spanning three district court decisions before reaching the 9th Circuit, Bernstein is by far the more expansive of the two encryption cases. Daniel J. Bernstein was a professor in the Dept. of mathematics, statistics, and computer science at the university of Illinois at Chicago. As a doctoral student at the University of California, Berkeley, he developed a "zero-delay private-key stream encryptor" called "snuffle." Bernstein wished to publish a description of his encryption method via both a paper (containing analysis and mathematical equations) and multiple computer programs written in the "C" programming language. The content of this programming constituted the source code for Bernstein's encryption program.[49] However, at that time encryption software was listed under the ITAR's munitions control list. Consequently, the State Department labeled Snuffle as a munition under the ITAR and demanded that Bernstein acquire a license to "export" (publish, sell, or share online) any aspect of the program.[50] Thus began a legal battle lasting the better part of four years.

In response to the State Department's decision, Bernstein filed an action challenging the constitutionality of the ITAR's regulations on encryption technology, winning an initial holding from the district court that encryption source code was a form of expression protected by the First Amendment.[51] Subsequently, the district court granted Bernstein summary judgment on his First Amendment claims, holding the ITAR's encryption regulations as an invalid prior restraint on speech.[52] In the wake of Bernstein's victory over the oppressive ITAR regime, the Clinton administration coincidentally shifted export control of commercial encryption from the Department of State

47 Junger v. Daley, 8 F. Supp. 2d 708 (N.D. Ohio 1998), *rev'd*, 209 F.3d 482 (6th Cir. 2000).

48 Bernstein v. U.S. Dep't of Justice, 176 F.3d 1132, 1136 (9th Cir.), reh'g granted, opinion withdrawn, 192 F.3d 1308 (9th Cir. 1999). [Hereafter, Bernstein v. Dep't of Justice].

49 *Id*. at 1136.

50 *Id*.

51 Bernstein v. U.S. Dep't of State, 922 F. Supp. 1426 (N.D. Cal. 1996). [Hereafter, Bernstein I].

52 Bernstein v. U.S. Dep't of State, 945 F. Supp. 1279 (N.D. Cal. 1996). [Hereafter, Bernstein II].

(ITAR) to the Department of Commerce (EAR). The Department of Commerce then created EAR regulations to govern the export of encryption technology.[53]

In an epic show of audacity, Bernstein then amended his complaint to add the Department of Commerce as a defendant, making the same constitutional claims against the EAR's export regulations.[54] Once again, the district court granted summary judgment in Bernstein's favor, finding the EAR regulations facially invalid as a prior restraint on the freedom of expression.[55] The Department of Commerce then appealed the district court's decision, leading to a holding from the 9th circuit court of appeals.

Although the EAR's regulation was theoretically less restrictive than previous ITAR regulations, the circuit court observed that any encryption falling within the coverage of the EAR required a prepublication license prior to an "export."[56] An export included publishing encryption software using any global medium, including the internet, if such publication would allow access by a foreign national.[57] The regulations held that printed materials containing encryption source code did not require a license; however the same source code would require a license if included on "machine-readable media," like CD-ROMs. Furthermore, even printed source code required a license if the printed material could be easily scanned and uploaded onto a computer.[58]

This overt ambiguity continued into the actual licensing process. For any export of encryption technology, the EAR took a "case-by-case" analysis to determine whether the export was "consistent with U.S. national security and foreign policy interests."[59] A license application was then sent to the president no later than 90 days after its submission; however, the regulations stated no limit as to how long the President could pocket the application. If the President eventually returned a negative verdict, an applicant had the right to administrative appeal only "within a reasonable time."[60] Furthermore, any final administrative decision was not subject to judicial review.[61]

In defense of the EAR's licensing system, the Government argued that encryption source code is different from other forms of expression because one can use it to directly operate a computer. Essentially, its functional

53 Bernstein v. U.S. Dep't of Justice, at 1135.
54 Bernstein v. U.S. Dep't of State, 974 F. Supp. 1288, 1292 (N.D. Cal. 1997). [Hereafter, Bernstein III].
55 *Id.*
56 Bernstein v. Dep't of Justice, at 1138.
57 *Id.*
58 *Id.*
59 *Id.*
60 *Id.*
61 *Id.*

aspects outweigh its expressive aspects.[62] However, the court held that, "this cannot be so . . . The First Amendment is concerned with expression, and we reject the notion that the admixture of functionality necessarily puts expression beyond the protections of the Constitution."[63] As to whether encryption source code constitutes expression, the court held;

> cryptographers use source code to express their scientific ideas in much the same way that mathematicians use equations or economists use graphs . . . mathematicians and economists have adopted these modes of expression in order to facilitate the precise and rigorous expression of complex scientific ideas . . . cryptographers utilize source code in the same fashion.[64]

Because encryption source code constitutes constitutionally protected expression, the court held that any licensing regime placing restrictions upon the dissemination of encryption source code is subject to facial challenge as a prior restraint;

> A licensing regime is always subject to facial challenge as a prior restraint where it **[1]** 'gives a government official or agency substantial power to discriminate based on the content or viewpoint of speech by suppressing disfavored speech or disliked speakers,' and has **[2]** 'a close enough nexus to expression, or to conduct commonly associated with expression, to pose a real and substantial threat of . . . censorship risks.[65]

Because prior restraints on speech and publication are "the most serious and least tolerable infringement on First Amendment Rights,"[66] the court applied a three-factor test to determine whether the EAR regulations constituted a valid prior restraint on encryption source code. For a licensing scheme to impose a valid prior restraint on expression, the court held it must satisfy the following three factors: (1) any restraint must be for a specified brief period of time; (2) there must be expeditious judicial review; and (3) the censor must bear the burden of going to court to suppress the speech in question and must bear the burden of proof.[67] After applying these three factors to the EAR's regulations on encryption, the court found that there was no time limit governing when the President had to return a verdict on applications, and

62 *Id*. at 1142.
63 *Id*.
64 *Id*. at 1141.
65 *Id*. at 1139. (*Quoting* Lakewood v. Plain Dealer Publishing Co., U.S. 750, 759, (1988)).
66 *Id*. at 1142. (*Quoting* Nebraska Press Ass'n v. Stuart, 427 U.S. 539, 559, 96 S.Ct. 2791 (1976)).
67 *Id*. at 1144.

there was no firm time limit governing the internal appeals process.[68] Therefore, the court found that "the challenged regulations allow the government to restrain speech indefinitely . . . and as a result, Bernstein and other scientists have been effectively chilled from engaging in valuable scientific expression."[69] The court's holding was a major victory not only for Bernstein and his Snuffle program, but also computer programmers, encryption users, and political activists around the world.

However, the court didn't stop there. In addition to liberating encryption source code from a First Amendment standpoint, Judge Fletcher also takes several first steps down a path to protecting the free use of encryption for years to come. She first recognized that the science of cryptography "has blossomed in the civilian sphere, driven on the one hand by dramatic theoretical innovations within the field, and on the other by the needs of modern communication and information technologies."[70] In response to these communication and information needs, she stated, "It is the cryptographer's primary task to find secure methods to encrypt messages, making them unintelligible to all except the intended recipients."[71] Here, Judge Fletcher distinguished the critical difference between general encryption and encryption that actually works. The fact that a particular source code satisfies one's definition of "encryption technology" does not necessitate said technology's ability to protect private information. In regards to the importance of privacy, Judge Fletcher states;

> The government's efforts to regulate and control the spread of knowledge relating to encryption may implicate more than the First Amendment rights of cryptographers. In this increasingly electronic age, we are all required in our everyday lives to rely on modern technology to communicate with one another. This reliance on electronic communication, however, has brought with it a dramatic diminution in our ability to communicate privately.[72]

As Judge Fletcher was writing this opinion in 1999, cell phones were a fairly new and bulky commodity, email had only recently begun to overtake snail mail, and the monstrous social media industry was not even a twinkle in Mark Zuckerberg's eye. Unlike today's world, where smart phones and social media apps shape everything from how we grocery shop to who we elect as President. Nearly two decades ago, Judge Fletcher could already see the importance of encryption far beyond mere source code printed in university textbooks. In the court's holding, she writes that the free use of encryption

68 *Id.*
69 *Id.* at 1145.
70 *Id.* at 1137.
71 *Id.*
72 *Id.* at 1145.

likely involves not only the freedom of expression guaranteed under the First Amendment, but also the right of privacy secured by the Fourth Amendment;

> The availability and use of *secure* encryption may offer an opportunity to reclaim some portion of the privacy we have lost. Government efforts to control encryption thus may well implicate not only the First Amendment rights of cryptographers intent on pushing the boundaries of their science, but also the constitutional rights of each of us as potential recipients of encryption's bounty, viewed from this perspective, the government's efforts to retard progress in cryptography may implicate the Fourth Amendment, as well as the right to speak anonymously.[73]

Although the circuit court subsequently held that the case be reheard by the court *en banc* and withdrew its opinion,[74] Judge Fletcher's forward thinking set a strong precedent for future adjudication of regulatory issues involving encryption technology.

3.2 Junger v. Daley

Peter Junger was a professor at the Case Western University School of Law, maintaining sites on the internet that included information about his "computers and the law" course. Junger wished to post source code on his website demonstrating how computers work; however, at the time, such a posting was defined as an export under EAR regulations.[75] Junger submitted three applications to the Commerce Department requesting determinations of commodity classifications for encryption software programs and other items. Although the Commerce department found that printed source code in the first chapter of Junger's "computers and the law" textbook was allowable, his other submissions of various software programs were not allowable without a license.[76] Consequently, Junger filed an action to make a facial challenge to the Regulations on First Amendment grounds, seeking declaratory and injunctive relief that would permit him to engage in the unrestricted distribution of encryption software through his web site.[77]

Following in the footsteps of Bernstein, the 6th Circuit held that, "the issue of whether or not the First Amendment protects encryption source code is a difficult one because source code has both an expressive feature and a functional feature."[78] However, "the fact that a medium of expression has a functional capacity should not preclude constitutional protection."[79] Quoting

73 *Id*. at 1146.
74 Bernstein v. U.S. Dep't of Justice, 192 F.3d 1308 (9th Cir. 1999).
75 Junger v. Daley, at 483.
76 *Id*. at 484.
77 *Id*.
78 *Id*.
79 *Id*.

the Supreme Court in Roth v. United States, the court in Junger states, "'all ideas having even the slightest redeeming social importance," including those concerning 'the advancement of truth, science, morality, and arts' have the full protection of the First Amendment."[80] However, subsequent to the oral arguments presented for this case, the Department of Commerce amended the EAR to relax license requirements for encryption technology. This forced the 6th Circuit to reverse and remand the case for further consideration, pending whether Junger's constitutional standing survived the EAR's amended regulations.[81] Regardless of this hiccup in the adjudication process, the 6th Circuit's opinion helped further solidify encryption source code's status as a form of protected speech under the First Amendment and reinforced that expression and utility can walk hand-in-hand.

For those encryption advocates hoping to find a sense of security in federal circuit court jurisprudence, Junger and Bernstein provide a mixed bag of results. On one hand, freely available encryption source code appears safely within the protection of the First Amendment, expression/utility can co-exist, and the Government is barred from chilling scientific discussion. On the other hand, these cases were adjudicated nearly twenty years ago, involved antiquated encryption technology, and neither of the courts' holdings are truly final. Additionally, Judge Fletcher's analysis of encryption's potential Fourth Amendment implications is in dire need of elaboration. Taking into account both the positive and negative results of these cases, one is left standing on a proverbial ice berg: safely afloat for now, but for how long?

4. The Export Administration Regulation

Now that Harry and Ginny have QKD capabilities (thanks to Dobbie), they are able to communicate without fear of unwanted observation by Severus (for now). Because of this technological success, Dobbie is quite proud of his handy invention and wishes to share the technology with the world—both by freely publishing the source code + object code for his QKD device on the internet, and also by selling hardware components capable of using his code to transmit secret quantum-entangled keys. Having studied the Curcuit Courts' opinions in Bernstein and Junger, Dobbie now seeks to discover whether he will encounter any regulatory roadblocks when distributing his products. In general, the EAR is a dense, convoluted corn maze; a maze riddled with notes, notes to notes, and complicated exceptions. Nonetheless, to help Dobbie with his investigation, the next section of this paper will briefly summarize EAR regulations currently in place for encryption technology and analyze what protections/restrictions are in place for both

80 Junger v. Daley, at 484; (*Quoting* Roth v. United States, 354 U.S. 476, 484 (1957)).
81 *Id*. at 485.

conventional cryptography and future technology like quantum key distribution.

Generally, the EAR regulates items listed under its Commerce Control List (CCL) in adherence to the United States' obligations under the Wassenaar Arrangement.[82] Category 5, Part 2 of the CCL lists all regulated items associated with cryptography in sections 5A002, 5A992, 5A004, 5B002, 5D002, 5D992, and 5E002.[83] These sections of the list include "cryptography for data confidentiality having in excess of 56 bits of symmetric cryptographic strength key length," items "designed/modified to enable, by means of 'cryptographic activation,' an item to achieve/exceed [56 bits]," and items "designed/modified to use or perform 'quantum cryptography (Quantum Key Distribution – QKD).'"[84] These three item descriptions alone encompass a vast percentage of encryption technology, including encryption source code, software like PGP, and QKD capable hardware. Because any item on the list requires a license to export, it appears there is a radical disconnect between the Circuit Court's decisions in Junger/Bernstein and current EAR regulations However, CCL's broad regulatory umbrella comes with a number of notable exceptions; the most important of which offer apparent regulatory breaks for (**1**) published items,[85] (**2**) mass market items,[86] and (**3**) items falling under license exception ENC.[87]

4.1 Published Items

15 C.F.R. § 734.7(a) states that, "unclassified 'technology' or 'software' is 'published,' and is thus not 'technology' or 'software' subject to the EAR, when it has been made available to the public without restrictions upon its further dissemination" in a number of ways, including: in libraries, at conferences, on the internet, in written manuscripts, computer readable datasets, at open gatherings, and for researchers of fundamental research.[88] However, § 734.7(b) appears to directly contradict itself, stating that this exception does not apply to encryption object code software (primarily functional code)[89] unless it's corresponding source code (primarily expressive

82 15 C.F.R. § 742.15 (2016); *The Wassenaar Arrangement*, INT'L INST. OF STRATEGIC STUD. 1, (August, 1996).

83 *See* Appendix A; Bureau of Industry and Security: Quick Reference Guide Category 5 Part 2 – Information Security: ECCN 5X. *Available at* https://www.bis.doc.gov/index.php/documents/new-encryption/1652-cat-5-part-2-quick-reference-guide/file. (last visited April 19, 2018); *see also*, 15 C.F.R. Pt. 774, Supp. 1, Cat. 5 (2017).

84 *Id*.

85 15 C.F.R. § 734.7 (2016).

86 15 C.F.R. Pt. 774, Supp. 1, Cat. 5, Part 2, Note 3 (2017).

87 15 C.F.R. § 740.17 (2017).

88 15 C.F.R. § 734.7 (2016).

89 Bernstein v. Dep't of Justice, at 1142. Derived from source code, object code is directly controls the functioning of a computer.

code)[90] meets the prepublication criteria set out in section 742.15(b).[91] This section once again states that encryption source code made publicly available is not subject to the EAR; however, "you must notify BIS and the ENC Encryption Request Coordinator via email of the Internet location (e.g., URL or Internet address) of the publicly available encryption source code."[92] What we are left with is that both directly functional object code and expressive source code are essentially free from the EAR's grasp, on the condition that exporters of encryption software notify both the BIS and the NSA of where software is made available on the internet. Perhaps this is a small price to pay for "freedom?"

4.2 Mass Market Items

Another way to avoid needing an EAR license for encryption technology is to sell it. Note 3 to category 5, part 2 of the CCL states that encryption software falling under 5A002 and 5D001(a)-(b)[93] is not controlled by the EAR if made "generally available to the public by being sold, without restriction."[94] This exception applies to a majority of encryption tech, expressly *excluding* items associated with QKD. However, in order for an item to be exempt under the mass market exception, 15 C.F.R. § 740.17(b) demands that the exporter submit either a yearly self-classification form (essentially a statement identifying the technology) or a one-time classification request (similar to the self-classification form, only with a 30 day holding period).[95] After successfully completing whichever of these two classifications is required for a particular product, the majority of commercial encryption items are ready to be sold around the world.

4.3 License Exception ENC

Despite the arguably broad umbrella of the Published Item and Mass Market exceptions, several encryption technologies remain un-exempted; most notably, items associated with quantum encryption. Thankfully, License Exception ENC takes the reigns, providing that quantum cryptography may be exported without a license after the exporter submits (1) a classification request to BIS,[96] and (2) a semi-annual sales report[97] detailing the product's

90 Bernstein v. Dep't of Justice, at 1142. "The distinguishing feature of source code is that it is meant to be read and understood by humans, and that it cannot be used to control directly the functioning of a computer."
91 15 C.F.R. § 734.7(b) (2016).
92 15 C.F.R. § 742.15(b) (2016).
93 *See* Appendix A.
94 *Supra*, note 84.
95 15 C.F.R. § 740.17(b) (2017).
96 *Supra*, note 87; see also Classification Request Guidelines, BIS.GOV, *available at* https://www.bis.doc.gov/index.php/licensing/commerce-control-list-classification/classification-request-guidelines. (Last visited May 1, 2018).

dissemination.[98] Upon submission of its classification request, a product becomes immediately eligible for export to a host of countries.[99] After 30 days, the product becomes eligible for export to nearly every country on Earth, save those labeled "terrorist nations."[100]

5. Quantum Key Distribution and the Future

Twenty-five years ago, cellular phones resembled cinder blocks, home computers were the size of a mini-fridge, and the internet was a finite landscape one could traverse over a weekend. As our needs developed, so did these technologies. Today, basic smartphones and laptops cruise the now infinite internet at warp-speed, utilizing computing power beyond that of our previous generation's wildest dreams. Encryption technology has also developed and adapted to changing times. Whereas PKC once stood as the bastion of secure communication, QKD now rises to take its place, necessitated by privacy concerns and catalyzed by revolutionary scientific research. Although cryptographers once spoke primarily through various computer code languages, they now speak the language of particle physics, sending and receiving entangled photons rather than computer code. To some, new languages seem foreign or even scary; nonetheless, just because something appears different does not mean it should be treated as such. It is this author's position that quantum encryption is the natural evolution of traditional encryption—a product of both the consumer's need for effective information security and the progression of scientific expression and exploration. This new "smartphone" of cryptography deserves equal or better protection than that afforded to traditional "cinder-block" forms of cryptography.

5.1 Key Points from Junger/Daley

Whether by sheer coincidence or strategic planning, the federal government managed to defer a final judgment in both Junger and Bernstein by actively shifting and amending language in the EAR. Although the absence of true final holdings is not ideal for encryption advocates, the court in both cases provided a modest well-spring of language protecting the free use and distribution of encryption source code. If applied analogously to QKD, this same language becomes an arsenal for protecting encryption technology going into the future.

97 How to File an Semi Annual Sales Report, BIS.GOV, *available at* https://www.bis.doc.gov/index.php/policy-guidance/encryption/4-reports-and-reviews/b-semi-annual-sales-report. (last visited May 1, 2018).

98 *Id.*

99 15 C.F.R. § Pt. 740, Supp. 3 (2016).

100 15 C.F.R. § 740.17(b) (2017).

For example, the court in Bernstein expressly rejected the notion that "the admixture of functionality necessarily puts expression beyond the protections of the Constitution."[101] In the same way that the court analogized cryptographers' use of source code to mathematicians' use of equations, modern cryptographers' use of QKD-capable software/hardware should be analogized to the use of traditional source code: a method by which scientists facilitate the "precise and rigorous expression" of scientific ideas.[102] Similarly, the court in Junger held, "the fact that a medium of expression has a functional capacity should not preclude constitutional protection."[103] It is this author's stance that, because QKD has far more than a slight "redeeming social importance" and concerns "the advancement of truth, science, morality, and arts," it should have the full protection of the First Amendment.[104] Although QKD may sound futuristic and foreboding due to the over-saturation of sci-fi television with words like "quantum," It is a beacon of hope for entrepreneurs, major businesses, and social/political advocates around the world relying on access to secure communication methods.

On the topic of security, Judge Fletcher emphasized that the cryptographer's primary task is to develop *secure* encryption methods, "making them unintelligible to all except the intended recipients."[105] Twenty-five years ago, programs like OpenPGP embodied this pursuit; however, modern technological developments demand that practitioners of free speech and scientific expression adopt secure communication on the quantum level. Judge Fletcher expressly stated the importance of fighting "to reclaim some portion of the privacy we have lost," and posited that the free use of encryption implicates not only the freedom of expression guaranteed by the First Amendment, but also the right to privacy guaranteed by the Fourth Amendment.[106] Because of the fundamental nature of these rights, the court in Bernstein held that any licensing scheme imposing a restraint on the freedom of scientific expression must satisfy three factors: (1) any restraint must be for a specified brief period of time; (2) there must be expeditious judicial review; and (3) the censor must bear the burden of going to court to suppress the speech in question and must bear the burden of proof.[107] This three-part test provided a sufficient legal standard to protect Bernstein's right to freely export encryption source code. If applied to modern day QKD, the same legal standard could serve as a moat surrounding the genesis of a QKD-capable society.

101 *Supra*, note 63.
102 *Supra*, note 64.
103 *Supra*, note 79.
104 *Supra*, note 80.
105 *Supra*, note 71.
106 *Supra*, note 73.
107 *Supra*, note 67.

5.2 Key Points from the EAR

As previously shown, QKD technology is regulated relatively lightly under current EAR language. Exporting QKD under license exception ENC requires the submission of a (1) a classification request to BIS, and (2) a semi-annual sales report detailing the product's dissemination.[108] No, these requirements are not as severe as those faced by Bernstein and Junger in the mid 1990s; however, the prepublication requirements for QKD are more numerous and onerous than for conventional encryption. Because QKD technology is the natural evolution of conventional encryption methods, it is this author's position that QKD should share the same regulatory shelters as conventional encryption listed under section 5A002(a) of the CCL. Designating QKD under section 5A002(c) of the CCL sets it apart from encryption as a whole, exposing it to potential regulatory actions by lawmakers who neither understand nor have an interest in the future of QKD. Therefore, the EAR should be amended to include QKD under 5A002(a), moving it under the umbrella of both the published item[109] and mass market item[110] exceptions to the EAR. By designating QKD under 5A002(a) of the CCL, it would receive the same protections as traditional encryption methods and ensure the free development, use, and dissemination of this important technology.

6. Conclusion

When the Department of State transferred encryption technology over to the Department of Commerce, Bernstein could have saved himself years of intense strain and effort by simply dropping his case and waiting to see how the new regime would respond to his requests. However, he immediately took pre-emptive action to protect his freedom of expression. As a society on the verge of a quantum revolution, we must also take pre-emptive steps to protect this evolution of scientific expression. Conducting routine, preventive maintenance on a vehicle is always less expensive than replacing it outright. In the same way, taking action to surround quantum encryption with judicial and regulatory protections today could save years of difficult litigation in the future. One who does not exercise his/her rights loses them, and it is this author's belief that QKD should be free to develop, use, and export—in the name of scientific advancement, freedom of expression, and secure communication.

108 *Supra*, notes 95, 96.
109 *Supra*, note 84.
110 *Supra*, note 85.