Encryption and the Speech Surplus: Building a Backdoor to the First Amendment

Tuesday, March 28, 2017
Law Student Writing Competition Winner

Last August, China’s quantum satellite, Micius, flared into space, marking a new era in the encryption technology race. The satellite, which is said to be the first of its kind, harnesses the power of quantum mechanics to facilitate hack-proof communications. Quantum communications is still in its nascent stages of development, but if Micius proves successful, China’s space program would rightfully be considered the apogee of cryptographic achievement.

Meanwhile, in the United States, the Government is attempting to force domestic technology firms to weaken their encryption technology. Specifically, the Government is requesting technology firms such as Apple and Google to install so-called “backdoors” into their devices as a means of granting law enforcement officials access to encrypted devices that may contain information that is relevant to a criminal investigation. Apple and others have vehemently opposed these requests.

The prelude to this controversy began in December 2015 with the San Bernardino terrorist massacre. After the shooting that injured 22 and killed 14 occurred, the FBI recovered the shooter’s iPhone 5C, which was equipped with Apple’s iOS 9 operating system. Despite obtaining a search warrant, the FBI was unable to search the phone because it was locked with a user-determined numeric passcode. The FBI was prevented from manually entering random passcode guesses because Apple’s operating system was coded with a user-enabled auto-erase function that would have, if turned on, destroyed the phone’s contents after 10 erroneous attempts at the passcode. Another non-encryption-based feature that prevented the Government from entering passcodes on the phone’s screen was Apple’s “delay-upon-failure function,” which forces the user to wait a period of time after each failed passcode entry before making another attempt, up to an hour after the ninth failed attempt.

As a result of this technological impediment, the Government filed an injunction against Apple ordering the company to assist the FBI in their search of the phone. The assistance the Government sought from Apple was three-fold. First, the Government asked Apple to ensure that the auto-erase function on the shooter’s device was turned off. Second, it asked Apple to create a custom software system that would allow the Government to remotely enter passcodes by electronic means, instead of manually on the iPhone’s screen. Finally, the Government asked Apple to disable any additional time delay features between failed passcode attempts beyond those that exist on the phone’s hardware.

The case was eventually withdrawn because a third party was able to decrypt the files on the phone for the Government. But the case’s resolution did not quell the Government’s concern over the impenetrability of Apple’s encryption software. The struggle rages on, with the Government insisting upon the creation of a backdoor to their encryption system.
software program that would allow it to use “brute force” to hack into select encrypted devices.\(^{[16]}\)

If this request were granted, serious constitutional issues would arise. Strengthening the Government’s surveillance power by undermining encryption technology has clear Fourth Amendment implications.\(^{[17]}\) Less obvious, however, is the substantial harm that this regulation would inflict on the First Amendment. The judiciary should protect encryption technology against this regulation because encryption is a subtle, yet effective, tool for promoting free speech values while stemming the inflating costs of speech in the Internet age.

**Privacy Promotes Democracy**

Robert Post suggests that First Amendment coverage extends to forms of interactions that realize First Amendment values.\(^{[18]}\) He also argues that objects that normally receive no First Amendment coverage can find constitutional shelter once integrated into First Amendment media.\(^{[19]}\) By protecting the privacy of our conversations over the Internet, a recognized medium of expression, encryption source code serves several First Amendment values, and should, therefore, be afforded First Amendment coverage.

Democracy may be the most important value that encryption technology, through its ability to protect the privacy of communications, helps to serve. The integral role that privacy plays in maintaining the integrity of our democratic system was put on full display in the 2016 presidential election. United States intelligence officials firmly believe that the Russian Government compromised the emails of American political organizations with the intent to interfere with the United States election process.\(^{[20]}\) Wikileaks’ release of hacked emails from Clinton campaign Chairman John Podesta’s Gmail account cast a pall over Clinton that many believe harmed her election efforts.\(^{[21]}\)

So concerned was President Obama that the American political system was atrophying under the grip of cybercriminals that he ordered the intelligence community to conduct a “full review” of “malicious cyber activity” timed to United States elections dating back to 2008, when China was discovered to have hacked the Obama and McCain campaigns.\(^{[22]}\) The President was especially concerned about the country’s response to Russia’s hacking.\(^{[23]}\) In an interview, he called on the American people to reflect on what the country’s “obsession” with the leaks, which in his view contained “routine stuff,” said about “how our democracy is working.”\(^{[24]}\) In his words, “these emails got a lot more attention than any policy that was being debated during the campaign.”\(^{[25]}\)

The Court has shown reluctance to extend protection to private statements that bear on issues of “public importance.”\(^{[26]}\) In *Bartnicki v Vopper*, the president of a local teacher’s union told his chief negotiator during a cell phone conversation that if the school board doesn’t accept their proposal, they would have to go to their homes “to blow off their front porches.”\(^{[27]}\) The conversation was illegally intercepted and eventually made its way to a local broadcaster, who played it on his radio show.\(^{[28]}\) When the union president invoked state and federal laws prohibiting the disclosure of unlawfully intercepted information, the Court held the statutes unconstitutional in situations in which the persons that disclosed the information played no role in the illegal acquisition of the material.\(^{[29]}\) In its decision, the Court emphasized that the conversation implicated “the core purposes of the First Amendment” because it related to a matter of public concern.\(^{[30]}\)

The problem with the Court’s reasoning in *Bartniki* is that it underestimates the distorting effect that out-of-context statements can have on political discussions.\(^{[31]}\) The union’s president was obviously speaking hyperbolically when he said he wanted to blow off his opponent’s porches.\(^{[32]}\) But the radio host blew the importance of the union president’s jocular statements out of proportion by broadcasting it for three days straight just like it did during the 2016 election, sensationalism redirected listeners’ focus from important issues and toward more trifling ones, such as the union president’s alleged propensity to “do some work on...guys.”\(^{[34]}\)

The Court’s willingness to protect the disclosure of misappropriated information relating to issues of public concern is particularly problematic because democratic participation often takes place in intimate settings.\(^{[35]}\) An overly protective approach toward disclosure can have the effect of altering the content of private conversations.\(^{[36]}\) For these reasons, the privacy of our communications should be given greater protections.

It cannot be denied, however, that privacy sometimes conflicts with national security.\(^{[37]}\) ISIS used Telegram to take credit for the November 2015 terrorist attack in Paris.\(^{[38]}\) One law professor described privacy as a disease that afflicts government because of its tendency to impede quick responses to security threats.\(^{[39]}\) Richard Posner asserted that the rising risk of terrorism endangers society in such a way that creates a compelling government need to gather and search vast amounts of personal information.\(^{[40]}\)
Still, privacy should be protected when it produces the best outcomes for society. In the context of the encryption source code debate, privacy should prevail because encryption not only helps promote First Amendment values; it helps deter First Amendment costs.

**The Rising Costs of Speech**

**The Marketplace: A Flawed Analogy**

The motif underlying First Amendment jurisprudence is the Court’s unwavering assertion that “more speech is good.” In the marketplace of ideas, where speech is uninhibited, truth and freedom shall prevail, so the theory goes. What the Court fails to consider with its marketplace analogy, however, is the fact that speech, like any commodity in any marketplace, is subject to the Law of Diminishing Returns. The utility derived from an increasing factor of production may steadily climb over time, but at some critical point this utility begins to decline, at which point the costs associated with that factor of production begin to increase. The major flaw with the Court’s analysis of First Amendment issues in recent years has been its failure to account for the rising costs of speech imposed by technology.

**Disclosure as a Case Study**

The increasing cost of speech can be seen through disclosure, the form of speech that involves revealing something about someone else. The mere specter of disclosure carries significant costs. When it is not controlled, the threat of disclosure inflicts an exorbitant cost on our speech-infrastructure by discouraging individuals from participating in the exchange of ideas, thereby “chilling” speech. The threat of disclosure is largely a function of three variables – the sensitivity of information vulnerable to disclosure, the amount of information vulnerable to disclosure, and the probability of disclosure. Increasing any of these variables heightens the threat of disclosure. Before the information revolution, these variables were mostly under control, and as a result, so were disclosure-related costs.

Consider life during colonial America. One of the greatest threats to one’s privacy at this time was the threat that an individual would stand under the eaves of one’s home and listen to the conversations occurring inside, the offense from which the term “eavesdropping” was born. Eavesdropping during colonial times was certainly an intrusive act. The home had historically been held as a rare place of refuge where Americans could engage in intimately private affairs while confident that such activities would be shielded from prying eyes. Therefore, if successful, a colonial eavesdropper had the potential to misappropriate highly sensitive information.

But certain realities limited the overall threat that eavesdropping posed during early American times. To begin, the amount of information that a colonial eavesdropper could steal and disclose was limited to the amount of information the eavesdropper’s memory could hold. Moreover, while parroting the contents of another’s conversations can damage one’s reputation, hearsay generally does not possess as indicting of an effect as audio or visual evidence does. Several other factors limited the probability of disclosure. Eavesdropping necessarily required the act of standing next to someone’s house, the exposure of which likely deterred many from participating in the venture. Also, colonial eavesdropping’s physical presence requirement likely limited the number of possible perpetrators to those living in or near one’s community. Finally, social pressures could have discouraged people from disclosing information attained through the act of eavesdropping.

When the threat of disclosure is small, as it was during colonial times, there is little cause to be concerned that prioritizing disclosure over privacy will induce a systemic fear that manifests itself as widespread silence. Indeed, it may even be prudent to choose disclosure over privacy under such conditions. There is a reason why speech on matters relating to the personal lives of others, or in other words, gossip, has been observed in every culture known to mankind. Gossip helps reinforce positive community values and change others that are more harmful. As long as eavesdroppers pose an insignificant threat of disclosure, and therefore an insignificant cost on the right to free speech, society is arguably best served by admitting their occasional heist into the marketplace of ideas.

Technology, however, has spawned an advanced eavesdropper, unfettered by the physical limitations of the past. As Warren and Brandeis observed in their seminal paper on privacy, “The Right to Privacy,” the invention of the “snap camera” gave the morbidly curious the ability to surreptitiously take pictures of others. This invention dramatically changed the type and amount of information about us that was vulnerable to disclosure. No longer did the eavesdropper have to rely on a faulty human memory to aggregate data about others; technology’s photographic memory allowed the eavesdropper to extract, store, and disseminate detailed visual depictions of his subject. Because of this reality, Warren and Brandeis advocated for a more vigorous approach to protecting
privacy. If the camera calls for the creation of broader privacy protection measures, then the Internet requires a total reformulation of privacy-related First Amendment doctrine. In recent years, almost every aspect of our daily lives has migrated from the physical world to the virtual one. Phone books, photo albums, libraries, diaries, and communication archives today are commonly stored online. Partially out of necessity and partially out of unquestioned habit, we upload an overwhelming amount of information about ourselves to the Internet. By centralizing our most personal information, the Internet has increased both the sensitivity and amount of information vulnerable to disclosure.

Making matters worse, the Internet has also elevated the probability of disclosure. As mentioned earlier, past physical limitations significantly narrowed the number of people that could carry out the act of disclosure to those that were in close proximity to the targeted information. Today's eavesdroppers, or hackers, however, do not need to physically press their ears against windows, or crouch behind bushes to steal information. A hacker can steal another's email history, medical records, financial information and identity while comfortably sitting behind a computer in Russia. Hackers are not deterred by the social pressures of the past, either. The anonymity provided by the Internet allows hackers to divulge highly personal information about others without fear that such disclosure will result in social retribution.

The Internet, the ultimate purveyor of speech, has enlarged the threat of disclosure to a state verging on ubiquity. This is just one way that the Internet has increased the costs of speech. If these rising costs continue to go undetected, and if speech is permitted to continue to flow freely, I suspect that we will eventually reach a critical mass of speech, at which point the unstable foundation upon which the First Amendment currently stands will crumble to the ground, and from talkative to taciturn we will turn.

**The Speech Bubble**

The economist Hyman Minsky offered a model that explains the nature of a typical financial crisis. A crisis is generally catalyzed by some sort of innovation that inspires great optimism among investors about the prospect of future growth in at least one sector of the economy. For the U.S. housing market in the early 2000s, the innovation was collateralized debt obligations and collateralized mortgage obligations. Recognizing an opportunity to profit from the innovation, banks expand the amount of credit that they lend. This initial investment powers production, increases demand, and leads to a wave of rising prices and profits. A positive feedback loop ensues in which these profits further inflame investor optimism, encouraging more investment and fueling greater profits.

At this point euphoria may develop. Fearing the possibility of missing out on an opportunity to make money, more and more people enter the marketplace, leading to overtrading and the formation of a “bubble.” Asset prices continue to appreciate until forward-looking investors begin to realize that the market value of their investment exceeds its actual value. These investors begin to sell, and when sales exceed purchases, a tense period follows in which asset prices hesitate from their upward trend and suddenly dip. This price hiccup invites presentiment, and more investors begin to rush for the exits. The result is generally a precipitous decline in prices and an implosion of the asset bubble.

Public discourse seems to be careening toward a similar crisis point. The information revolution was an exogenous shock that simultaneously opened new channels for the expression of feeble-minded ideas and stimulated our appetite for these thoughts. The marketplace is overheating. Twitter, Facebook, YouTube, Instagram, Yik Yak are just a few of the untold platforms available today for polemical prattling. As comedian Bo Burnham said, the Internet is “unrestrained, and anonymous, and horrifying, and violent, and quick, and too many people at once.” But website and television station operators will continue to finance our saturated speech market as long as it turns a profit. Meanwhile, unaccounted externalities are being passed to the consumer. The Supreme Court, like a central bank that refuses to acknowledge a blooming mania, is complicit in these rising costs. At some point, the costs of speech will outweigh its benefits, and gradually, or sharply, discourse will be chilled, and our bubble of free speech will implode. If speech is a commodity, I am selling short.

**The Way Forward**

Pointing out the problems of speech in the Internet age is easy; finding solutions has proven difficult. An unconventional idea that rose from the rubble of the worst financial crisis in American history may provide the direction we need.
Keynesian Speechonomics

The economic prosperity of the Roaring Twenties gave way to an irrational exuberance that transformed the staunchest prigs into profligates. The United States experienced a flood of income unlike anything it had ever seen. Unprecedented wealth motivated a well-meaning Herbert Hoover to say, “We shall soon with the help of God be within sight of the day when poverty will be banished from the nation.”

But the tide had turned by the late 1920s. Business enterprise, which generated $15 billion in wages, salaries and profits in 1929, generated just $886 million in 1932 – a fall of 94 percent. After the Great Depression, private investment stubbornly refused to recover.

Doubtful that business enterprise would dislodge the economy from stagnation, John Maynard Keynes offered a novel solution to the country’s lingering economic woes – government intervention. His suggestion was deemed heretical. Many condemned his prescription as an affront to the capitalist faith in the market’s ability to correct itself in the long run. To these people Keynes pithily replied, “In the long run we are all dead.”

Keynesian economics, once a subject of scoff, has had a lasting influence. European economies recognize the need for a strong government to provide generous welfare and education programs to assist those left behind by capitalism and globalization. Interestingly, the European approach to speech regulation is largely similar.

In contrast to the United States, European countries actively regulate public discourse. Rather than leaving their citizens equipped with nothing more than their freedom to either ignore or counter speech with more speech, European countries regularly repress harmful speech. In this age of rising speech costs, the Supreme Court’s passive regulatory approach is ill suited to uphold fundamental First Amendment values, such as dignity, equality and democracy. For this reason, the Court should emulate the European model and take a more affirmative role in its regulation of speech.

Admittedly, such a shift in policy would almost certainly be met with strong resistance. Just as government intervention in the economic affairs of the country in the 1930s was perceived to violate long-held notions of the role of government, speech regulation would likely be viewed in a similar way today. Moreover, certain regulations may even be counterproductive.

Reconsider disclosure. If the Court were to prohibit Wikileaks from disclosing the contents of Hillary Clinton’s hacked emails in an attempt to safeguard our democratic process, there would likely be a public outcry. Such an action would be perceived by many as an arrogation of the power to shape the contours of democratic discourse. Recognizing the opportunity to profit from a story ripe for sensationalism, one of several “news” outlets bereft of journalistic integrity would incite its audience to rebel against an alleged attack on the sacrosanct First Amendment right to free speech, causing a chain reaction of contempt for the Court and all beneficiaries of its decisions. Thus any attempts to curb the costs of speech will have to be executed with great delicacy.

Hidden Solution

A subtle way the Court could regulate speech costs without fomenting the furor of the First Amendment faithful is by protecting encryption technology. Strong encryption protects the privacy of information just as laws prohibiting disclosure do. Unlike an outright suppression of disclosure, however, a strong encryption stance would not create the impression that the Court is breaking with tradition by taking an activist role in its regulation of speech. When encryption performs its intended function of preventing disclosure, gossipmongers lose their speech infringement claims because they have lost the subject of their speech.

Encryption is just one measure that should be taken to dike the flooding costs of speech. It may not even put too much of a dent in the deficit. In order to further protect First Amendment values without offending First Amendment tradition, both the judiciary and the legislature should explore other ways that technology can help prevent speech costs from rising. In the meantime, the Court should invalidate encryption export regulations, master keys, backdoor solutions and any other laws Congress passes that would have the effect of impeding cryptographic development.

Conclusion

The Government’s attempt to weaken encryption technology would harm First Amendment values, such as democracy. Instead of entertaining the idea of passing a law that would weaken encryption, Congress should assist the judiciary in an effort to protect these values while curbing the rising costs of speech by funding
programs devoted to advancing encryption.

The future of encryption lies at the subatomic level. China has established itself as the leader in the quantum encryption race with the launch of its quantum satellite. The United States needs to invest the talent and resources necessary to pull even before the strength of its communications infrastructure is eclipsed.


[2] See id. The satellite works by creating pairs of entangled photons and beaming one half of each pair to base stations in China and Austria. The laser used to beam the photons through space is unique in that its quantum state cannot be observed without changing it. As a result of this property, any attempts to intercept encryption keys encoded in the photons would be detected and would change the key.


[4] Id.

[5] Id.


[7] Id. at 3.

[8] Id.

[9] Id. at 7.


[12] Id.

[13] Id.


[15] Karen Freifeld, Q&A: Manhattan DA investigations chief Sachs on cybercrime, Reuters Legal, (November 18, 2016) (explaining need for Government access to specific devices and need for legislative solution to prevent arms race between Government efforts to access devices and private companies upgrading encryption).


Id.

The Daily Show with Trevor Noah: Interview with President Obama (Comedy Central television broadcast December 12, 2016).

Id.


Id. at 519.

Id.

Id. at 529.

Id. at 533, 534.


Id.

Id. at 2137.

Bartnicki at 519.

Daniel Solove, Understanding Privacy, 143 (2008).

Id.

Id. at 93.


Solove, supra note 35, at 87 (recommending a pragmatic approach to weighing privacy’s harms against its benefits that involves expressing the value of privacy in terms of its practical consequences).

See Whitney v. California, 274 U.S. 357, 377, 47 S. Ct. 641, 649, 71 L. Ed. 1095 (1927). “If there be time to expose through discussion the falsehood and fallacies…the remedy to be applied is more speech, not enforced silence.”

United States v. Alvarez, 132 S. Ct. 2537, 2550, 183 L. Ed. 2d 574 (2012). “The theory of our Constitution is ‘that the best test of truth is the power of the thought to get itself accepted in the competition of the market,’” (quoting Abrams v. United States, 250 U.S. 616, 630, 40 S.Ct. 17, 63 L.Ed. 1173 (1919) (Holmes, J., dissenting)).

Richard W. Tresch, Principles of Microeconomics 126, 128 (8th ed. 2008). The marginal cost of output equals the change in total cost divided by the change in quantity produced (MC = ΔTC/ΔQ). The Law of Diminishing Returns ensures that the quantity produced will decline over time. Therefore, once diminishing returns take hold, the denominator in the equation above declines, and the marginal cost of output increases).

Solove, supra note 35, at 142.


[48] Commw. v. Lovett, 4 Pa. L.J. Rpts. (Clark) 226, 226 (Pa. 1831) (recognizing “eaves-dropping” as an actionable offense in Pennsylvania, but declining to find the defendant guilty because he was hired by man to spy on the man’s wife).

[49] William Blackstone, 4 *Commentaries* 223 (“The law has so particular and tender a regard to the immunity of a man’s house, that it styles it his castle, and will never suffer it to be violated with impunity”).

[50] *Amica Mut. Ins. Co. v. Kingston Oil Supply Corp.*, 134 A.D.3d 750, 21 N.Y.S.3d 318 (N.Y. App. Div. 2015) (“The ‘best evidence rule’ requires the production of an original writing where its contents are in dispute and are sought to be proven; the rule serves mainly to protect against fraud, perjury, and inaccuracies which derive from faulty memory”); See also 23 Mo. Prac., Missouri Evidence § 1000:1 (4th ed.) (discussing how many jurisdictions have extended the best evidence rule to recordings, photographs and videotapes).

[51] See Margaret Talbot, *The Attorney Fighting Revenge Porn*, The New Yorker, (December 5, 2016), http://www.newyorker.com/magazine/2016/12/05/the-attorney-fighting-revenge-porn. Carrie Goldberg, attorney who has devoted her career to protecting sexual privacy, opining that the Internet has given rise to more brazenly vindictive people: “Historically, we had checks and balances. If you are someone who is always seeking revenge, that’s going to affect your reputation. But on the Internet a guy can be really bad and his friends aren’t necessarily going to know...”


[55] Id. at 211-212 (noting that the doctrines of contract and trust were no longer sufficient to guard against harms caused by privacy infringements: “The narrower doctrine of [breach of contract] may have satisfied the demands of society at a time when the abuse to be guarded against could rarely have arisen without violating a contract or a special confidence; but now that modern devices afford abundant opportunities for the perpetration of such wrongs without any participation by the injured party, the protection granted by the law must be places upon a broader foundation”).


[57] Talbot, supra note 51, (quoting Goldberg).

[58] See note 73, infra.


[60] Id. at 27.

[61] Id. at 28.

[62] Id.

[63] Id.

[64] Id. at 28, 29.

[65] Id. at 29.

[66] Id. at 20, 30.
[67] Id. at 32.

[68] Id.

[69] Id.

[70] Id. at 33.

[71] See generally Clay Calvert, The Voyeurism Value in First Amendment Jurisprudence, 17 Cardozo Arts & Ent. L.J. 273 (1999) (discussing proliferation of reality television, talk shows and other vapid forms of entertainment, and Americans’ voyeuristic fascination with these shows).

[72] Bo Burnham, Bo Burnham on Political Correctness in Comedy, CBS News, (September 17, 2016), https://www.youtube.com/watch?v=D52TF1OtgSE.


[74] Robert L. Heilbroner, The Worldly Philosophers: The Lives, Times, and Ideas of the Great Economic Thinkers 248, (7th ed. 1999). “[Thorstein] Veblen…had fallen victim to the same dazzling lure that blinded America: when the most disenchanted of its observers could be tempted to swallow a draught, is there any wonder that the country was drunk with the elixir of prosperity?”

[75] Id.

[76] Id. at 248, 249.

[77] Id. at 274.

[78] Id.

[79] Id.

[80] Id. at 276. “Government spending was meant as a helping hand for business. It was interpreted by business as a threatening gesture.”

[81] Id. at 270 (discussing how the conclusion of Keynes’ The General Theory – that economies had no automatic safety mechanism – was dismaying at the time).

[82] Id. at 262.

[83] Id. at 286, 287 (noting that European economists never fully embraced Keynes but his ideas influenced their economies).


[85] Id.

[86] Heilbroner, supra note 74, at 277.


[88] Id. (predicting that regulations prohibiting racist speech would inspire more intense and widespread resentment for minorities because such a regulation would be viewed as an offense to the cherished right to free speech).
Many cases of disclosure don’t even involve hacking. Sometimes disclosure of sensitive material results from a betrayal of trust. See Talbot, supra note 51.

Of course, asking a government to use scientific advancements to prevent its citizens from inflicting harm on others is reminiscent of the plot of Anthony Burgess’ *A Clockwork Orange*. What lengths a government should go to manage the behavior of its populace is a topic that raises deeply philosophical questions relating to good, evil and free will that are outside of the scope of this paper. Consider, for example, Scottek, supra note 73, quoting Reddit’s CEO, “Virtuous behavior is only virtuous if not arrived at by compulsion.”

See Chin, supra note 1.


© Stephen Paul Byrnes

**Source URL:** https://www.natlawreview.com/article/encryption-and-speech-surplus-building-backdoor-to-first-amendment