Perceiving the “conceptual deficit”: effective policy for the Information Age

Helen Picard

A research paper submitted to the University of Dublin, in partial fulfillment of the requirements for the degree of the Master of Science, Interactive Digital Media

2016

Declaration

I have read and I understand the plagiarism provisions in the General Regulations of the University Calendar for the current year.

I have also completed the Online Tutorial on avoiding plagiarism, 'Read, Steady, Write'.

I declare that the work described in this research paper is, except where otherwise stated, entirely my own work and has not been submitted as an exercise for a degree at this or any other university.

Signed: _____

Helen Picard

13/05/2016

Permission to lend and/or copy

I agree that Trinity College Library may lend or copy this research paper upon request.

Signed: _____

Helen Picard

13/05/2016

Table of Contents

You know something is happening here, but you don't know what it is…Do you, Mr. Jones?"
- Bob Dylan, Ballad of a Thin Man

Seldom do more than a few of nature's secrets give way at one time.
- Claude Shannon, The Bandwagon

1. Introduction

The historical continuum that began with Claude Shannon has in 2016 arrived at a faceoff between technology and politics. Shannon kept meaning separate from communications systems, but meaning now exists in the ethical implications of modern encryption. This is because the proliferation of information technologies, concurrent to the blurring line between phones and computers, has caused the current legal regulation of encrypted communications to be a broader regulation of information itself.

In 1956, after founding Information Theory in 1948, Claude Shannon warned the academic community against interpreting communication technologies outside of mathematics. Decades later, information and information technologies have become inextricable with our society, culture, and politics. The historical continuum for information technologies beginning with Shannon's warning has reached maturation in the 2010s with our social, cultural, and political dependence on those same technologies. In other words, the debate over exceptional access to encryption, achieved via the design of communications systems, is a more ethical and existential one than the debate that took place at their advent in the 1950s with Claude Shannon's warning.

The two Crypto Wars demonstrates an inability to resolve our societal relationship to information technologies with effective policies. There has been a paradigm shift to a level of dependence on communications technologies that has outpaced our conscious relationship with them.

Information Theory is purely concerned with scientific applications and as such can only act as an ideological touchstone for the Crypto Wars, which deal with the social integration of the technologies of Information Theory. Policy and its cultural and social consequences, not the engineering of optimal technology or sheer scientific thinking, define the Crypto Wars. Conflicts of the Information Age go beyond Shannon's purely mathematical considerations of Information Theory's technologies towards a conceptual consideration. The "conceptual deficit"[1] that Luciano Floridi says is a by-product of our rapid "hyperhistorical"[2] paradigm shift into the Information Age must be filled by new modes of thinking that consider the newly blurred line between phones and computers, which is addressed in Chief Justice Robert's opinion in the 2014 Riley v. California case.

The Crypto Wars of the 1990s and 2010s pit politicians against technologists, who define the debate according to their own paradigms: security and rule of law (politicians) vs. privacy and reliable technology (technologists). Using Shannon's perspective as a point of origin and contrast, we can see the scale and complexity which communication technologies have reached in society, where one is dependent upon the other.

The "conceptual deficit" of our Information Age exists between these polar political and technologies ideologies, technology isolated from the politics of its societal use, that define the Crypto Wars. These ideological absolutes fail to recognize the co-dependence of their fundamental ideologies, and the possibility of effective policy for the Information Age has suffered.

---

[1] Luciano Floridi, *The Fourth Revolution: How the infosphere is reshaping human reality* (Oxford: Oxford University Press, 2014): ix.
[2] Floridi, *The Fourth Revolution,* 3-4.

While both have their own ethical code arising from their position in the Crypto Wars, neither the apolitical nature of technology, nor the impartial rule of law, can alone fill the conceptual deficit. What will set the tone for the Information Age and conclude the Crypto Wars is not purely "straight math," nor unchecked government surveillance, but a balanced technology that optimizes security and limits legal exceptional access on a principled basis. The Crypto Wars' imperfect grappling with technological integration shows that the deficit must first be recognized with coherent policy to follow. A first step towards coherent policy is perceiving our conceptual deficit and understanding that applied neutrality is rarely neutral.

Sustainable policy for and of the Information Age will follow the recognition of the conceptual deficit through new paradigmatic modes, like the blurring line between phones and computers. This embrace of the Information Age begins with conceptual paradigm shifts that redefine both technology and the law, like the 2014 Riley v. California case ruling.

This paper will review the main engagements of the two Crypto Wars, will consider the ongoing American debate over cryptography, including the recent flash-point, the 2016 FBI-Apple dispute, and will refer to legislative attempts to address fundamental policy issues such as the draft Compliance with Court Orders Act of 2016 (also known as the Burr-Feinstein Bill).[3] In addition, this paper will attempt to demonstrate that these disputes are gradual and imperfect attempts to deal with what Floridi describes as the hyperhistorical age in which we find ourselves. It follows that any principled resolution of the issues must rise above legacy concepts and assumptions, if a calibrated and effective result is possible. In order to have a "reality check" one must understand reality.

[3] Senator Richard Burr and Senator Dianne Feinstein, Compliance with Court Orders Act of 2016, Discussion Draft, released April 13, 2016, https://www.eff.org/document/burr-feinstein-encryption-bill-discussion-draft.

From Shannon's starting point, in the 21st century we now have Luciano Floridi's assertion that information has rendered us "hyperhistorical", dependent on and in a symbiotic relationship with information and information technologies. Apple's resistance to the FBI is based on the realization that more is at stake than technology in isolation from meaning. The Crypto Wars are a symptom of the gradual realization, the partially conscious and imperfect manner in which we are coming to grips with this new reality of the Information Age. In the same way that Shannon explained exactly what information was and was not for communications technologies we need to understand, politically and socially, the profound nature of this change for those same technologies and engage in a discussion that 'catches up' to where we are.

Lillian Ablon, a technology researcher for the Rand Corporation, has asserted that, "Instead of just letting the technology rush ahead of us and then trying to catch up in terms of privacy and security, we should be baking those things into the systems from the start."[4] Regardless of immediate context, Ablon is suggesting that policymakers should understand the larger context in which technological issues need to be considered, debated, and ultimately determined.

[4] Lillian Ablon, "Growing dependence on technology raises risks of malfunction," Crain's, July 9, 2015, http://www.crainsnewyork.com/article/20150709/TECHNOLOGY/150709895/growing-dependence-on-technology-raises-risks-of-malfunction.

2. Information: the theory, the age

2.0 The Theory

In his book *The Fourth Revolution*, Oxford philosophy professor Luciano Floridi describes modern networks as "a bit like having pumps and pipes made of ice to channel water: it is all H20 anyway."[5]

Floridi offers an evocative metaphor for modern networks. For example, how does a wireless signal deliver the specific information in a full episode of *House of Cards* with all the dialogue, colours, and pixels in the right place? The sound, the images, the protocol for delivering them to your computer, playing them on your computer, its unique identifications en route, are all coded information that any computer can interpret – both the channel's medium and its content. Hence, pipes of ice channelling water. Mathematical precision, specifically channel coding, allows wireless (and wired) signals to deliver information across a network of computers to your device.

Who pioneered such a conceptually subtle means of communication? Claude Shannon, a mathematician and electrical engineer who studied at the Massachusetts Institute of Technology (MIT), worked at Bell Laboratories, and most notably founded the field of Information Theory. Shannon invented not only channel coding, the "pipes of ice channelling water." Amongst many other things, he also invented the conceptual schematic for reliable communications systems.

Starting with his 1948 essay published in the *Bell Systems Technical Journal*, "A Mathematical Theory of Communication," Claude Shannon created the digital realm as we know it:[6]

[5] Floridi, 41.

> Before Shannon, communication engineers worked on their own distinct fields, each with its own distinct techniques: telegraphy, telephony, audio and data transmission all had nothing to do with each other.
>
> Shannon's vision unified all of communication engineering, establishing that text, telephone signals, images and film – all modes of communication – could be encoded in bits, a term that was first used in print in his article.[7]

Shannon brought multiple fields together under the same banner of Information Theory for use in communications systems.

Shannon reformulated the definition of information and quantified it. He made it into something quantifiable and useable for engineering communication systems.

Before Shannon, "information" was defined as subjective and intangible, not as a unit of measurement, or quantifiable part of an engineered system. Shannon re-purposed the definition of information and simplified it, allowing for its more complex mathematical applications. In Shannon's own words, a communications system simply reproduces a message from sender to receiver:

> Frequently the messages have *meaning*; that is they refer to or are correlated according to some system with certain physical or conceptual entities. These semantic aspects of communication are irrelevant to the engineering problem.[8]

For Shannon, information was defined by uncertainty, not as any possible message, but as the statistically likely message.[9] Key to applying this new definition of information was the understanding that its constituent messages were merely part of the engineered system, without subjective meaning or importance.

> Information Theory, as Shannon's work is called, defines information as the informational content of signals abstracted from all specific human information. It concerns not the question 'what sort of information?' but rather, 'how much

---

[6] Brian Winston, *Media Technology and Society, A History: From the Telegraph to the Internet* (London: Routledge, 1998), 153.
[7] Aftab, Cheung, Kim, Thakkar, Yeddanapudi, "Information Theory: Information Theory and the Digital Age," (Final paper, *Project History,* Massachusetts Institute of Technology, 2001): 5, http://web.mit.edu/6.933/www/Fall2001/Shannon2.pdf.
[8] Shannon, "*The Mathematical Theory of Communication* (Chicago: University of Illinois Press, 1949): 31.
[9] For more on this definition see Weaver's explanation of Shannon's quantification of information in "The Mathematical Theory of Communication," 8-16.

> information?' (Cherry 1961: 168). 'The word information, in this theory, is used in a special sense that must not be confused with its ordinary usage. In particular, information must not be confused with meaning' (Weaver and Shannon 1949: 11).[10]

In other words, drain the meaning from the information channelled by information systems. The communications system shown in Figure 1 necessitates information that is subject to the system's design. There is no alternate design for specific kinds of messages; there is only a universal and optimal design. Draining meaning from the message defuses the component messages, defuses the information, letting it flow like water.

> Information Theory was important to the Internet because Information Theory commoditises information, draining it of semantic content. Encoded electronically and treated as beings without meaning, messages became far more malleable than they were traditionally. [11]

The difference between the "pipes of ice" and the water they channel, both constituted by the same medium of information and made different by state, is achieved with Shannon's definition of quantified information (and channel coding).

Both applied mathematics and abstract systems of information are studied in Information Theory, but the famous diagram Shannon made as a general template for communications systems can be understood by non-mathematicians.[12]

[10] Winston, *Media Technology and Society,* 153.
[11] James Gleick, *The Information, A History, A Theory, A Flood* (New York: Knopf Doubleday Publishing Group, 2011): 216-217.
[12] Raymond W. Yeung, *A First Course in Information Theory* (New York: Springer, 2002): 5.

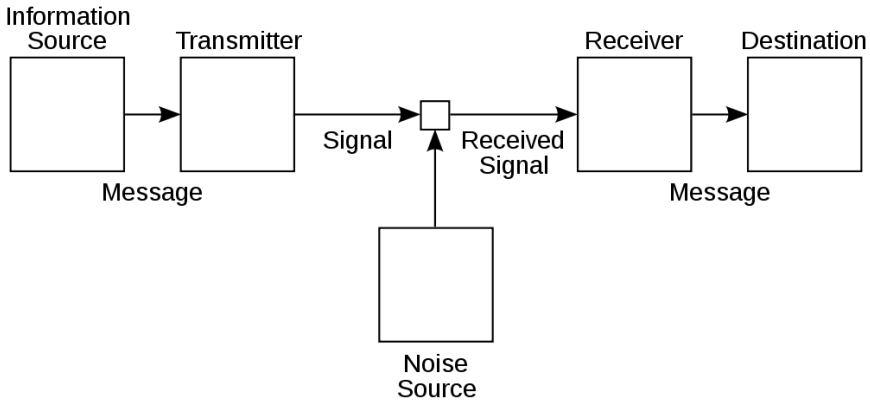

Figure 1: Claude Shannon, *Schematic diagram of a general communication systems*, in "A Mathematical Theory of Communication," *The Bell System Technical Journal* 27 (July, October 1948): 2, https://archive.org/details/bstj27-3-379.

The applications of Shannon's theories are mind boggling. In "Information Theory and the Digital Age" Aftab et al. say:

> Information theory has innumerable applications today. CDMA [Code-Division Multiple Access] is still being used and researched to improve voice and data communications systems. Modern applications of spread spectrum range from low speed fire safety devices to high-speed wireless local area networks. Storage devices, such as hard disks and RAM [Random Access Memory], also employ Information Theory concepts. Using Reed-Solomon codes for compression, and Hamming codes to correct errors, major breakthroughs have been made, allowing gigabit of information to be stored on inches of space.
>
> Information theory's long shadow falls over many more of the things that have become commonplace today. It has strongly influenced not only the development of wireless systems, CDs, and data storage, but also computer networks, satellites, optical communication systems, mobile phones, MP3s, JPEGs, and of course, the Internet.[13]

Some of the technologies Aftab uses, "Reed-Solomon codes," "CDMA," "Hamming codes," are beyond the scope of this essay. But any reader can appreciate the list of everyday technologies, mobile phones, satellites, high-speed wireless, and of course, the Internet.

As James Gleick, author of *The Information,* states,

[13] Aftab et al., "Information Theory: Information Theory and the Digital Age," 22-23.

> An invention even more profound and more fundamental [than the transistor, invented the same year, 1948] came in a monograph spread across seventy-nine pages of *The Bell System Technical Journal* in July and October. No one bothered with a press release. It carried a title both simple and grand—'A Mathematical Theory of Communication'—and the message was hard to summarize. But it was the fulcrum around which the world began to turn.[14]

Information Theory may have been the fulcrum around which the world turned in the 1950s, but it is not the fulcrum around which the Crypto Wars turned. These events could only have occurred because "meaning" was indeed relevant to Information Theory and its practical uses.

2.1 The Age

Information Theory's credo of neutrality towards information is not philosophical.[15] It is a defining tenet for the *engineering* of communication systems. It exists as a by-product of a scientifically optimal design. Nevertheless, it is a concept that applies to Information Theory technologies, those technologies that culminated in the advent of the Information Age.

However, in contrast to the purely neutral and formulaic characterization of information under Shannon's perspective, Floridi states that "recently … human progress and welfare [have] begun to be not just *related to,* but *mostly dependent on*, the successful and efficient management of the life cycle of information."[16]

---

[14] James Gleick, *The Information,* 4.
[15] James Gleick, author of *The Information,* himself avoids using the term "philosophical" to describe Shannon's theory. James Gleick, "The Information: A History, a Theory, a Flood | Talks at Google," March 17, 2011, YouTube video, 4:50, uploaded March 24, 2011, https://www.youtube.com/watch?v=iyOzSzcDwg8.
[16] Floridi, *The Fourth Revolution,* 3-4.

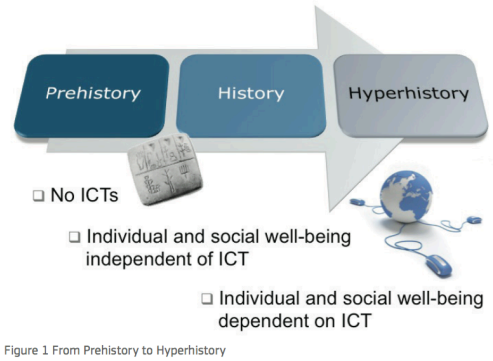

Figure 2. Luciano Floridi. *From Prehistory to Hyperhistory,* in "Hyperhistory and the Philosophy of Information Policies," an initiative of the European Commission, 4, https://ec.europa.eu/digital-agenda/sites/digital-agenda/files/Contribution_Floridi.pdf.

Floridi explains that we are currently in an Information Age,[17] a "hyperhistorical" time defined by and distinguished from previous historical eras by our dependence on information and communication technologies (ICTs).

> For example, all members of the G7 group—namely Canada, France, Germany, Italy, Japan, the United Kingdom, and the United States of America—qualify as hyperhistorical [informational] societies because, in each country, at least 70 per cent of the Gross Domestic Product (GDP, the value of goods and services produced in a country) depends on intangible goods, which are information-related, rather than on material goods, which are the physical output of agricultural or manufacturing processes. [18]

We are an informational society: "inforgs" living in an "infosphere." James Gleick chooses to describe us as "creatures of the information."[19] However Floridi or Gleick interprets our dependence on technology, its prevalence to our society cannot be ignored, nor can Shannon's contribution to its coming about. None of this could have occurred without a shift away from the information-neutral basis on which the Information Age was founded. This requires an examination of the move away from information

[17] This is a generally accepted statement, though there are alternate definitions of the Information Age. For more reading on the Information Age see: David S. Alberts and Daniel S. Papp, eds., "The Information Age: An Anthology on Its Impact and Consequences," CCRP Publication Series, 1997, http://www.dodccrp.org/files/Alberts_Anthology_I.pdf; James A. Dewar, "The Information Age and the Printing Press, Looking Backward to See Ahead," the Rand Corporation, 1998, http://www.rand.org/pubs/papers/P8014/index2.html; David S. Alberts and Richard E. Hayes, "Power to the Edge, Command…Control…in the Information Age," DoD Command and Control Research Program, CCRP Publication Series, http://www.dodccrp.org/files/Alberts_Power.pdf; Joseph Migga Kizza, Ethical and Social Issues in the Information Age (London: Springer-Verlag, 2010).
[18] Floridi, *The Fourth Revolution,* 4.
[19] Gleick, *The Information,* 426.

neutrality. Let us, as James Dewar says in his report, "The Information Age and the Printing Press," look backwards to see ahead.[20]

[20] James A. Dewar, "The Information Age and the Printing Press, Looking Backward to See Ahead," the Rand Corporation, 1998, http://www.rand.org/pubs/papers/P8014/index2.html

3. The 1950s, Shannon's Warning

3.0 The bandwagon's history: new fields, new farce

After Shannon published his 1948 paper, in the early 1950s a number of disciplines attempted to co-opt Information Theory.

James Gleick outlines the profound impact Information Theory initially had on the humanities. Academics convened conferences to discuss the application of Information Theory to their diverse fields. Shannon had a conservative reaction to this phenomenon:

> With psychologists, anthropologists, linguists, economists, and all sorts of social scientists climbing aboard the bandwagon of information theory, some mathematicians and engineers were uncomfortable. Shannon himself called it a bandwagon. In 1956 he wrote a short warning notice—four paragraphs: 'Our fellow scientists in many different fields, attracted by the fanfare and by the new avenues opened to scientific analysis, are using these ideas in their own problems…Although this wave of popularity is certainly pleasant and exciting for those of us working in the field, it carries at the same time an element of danger.' Information theory was in its hard core a branch of mathematics, he reminded them. He, personally, did believe that its concepts would prove useful in other fields, but not everywhere, and not easily: 'The establishing of such applications is not a trivial matter of translating words to a new domain, but rather the slow tedious process of hypothesis and experimental verification.' Furthermore, he felt the hard slogging had barely begun in 'our own house.' He urged more research and less exposition. [21]

An example of the movement that persisted in ignoring Shannon's warning was the "Conference on Cybernetics," attended by intellectuals from both the humanities and sciences.

The first meeting began on March 22nd, 1950, and lasted two days.[22] "Throughout the conferences, it became habitual to use the new, awkward, and slightly suspect term *information theory.* Some of the disciplines were more comfortable than others. It was far from clear where information belonged in their respective worldviews."[23]

---

[21] Gleick, *The Information*, 262
[22] Gleick, *The Information*, 243.
[23] *Ibid.*

Neurophysiologist Warren McCullough, who organized the conferences, was "a dynamo of eclecticism and cross-fertilization." As Gleick says, "A host of sciences were coming of age all at once—so-called social sciences, like anthropology and psychology, looking for new mathematical footing…"[24]

Most of the interpretations applied Information Theory's abstract structure, like the diagram included above, to the schema of their own fields.[25]

Weaver's description of Information Theory helps us understand its attraction to the humanities:

> This is a theory so general that one does not need to say what kinds of symbols are being considered – whether written letters or words, or musical notes, or spoken words, or symphonic music, or pictures. The theory is deep enough so that the relationships it reveals indiscriminately apply to all these and to other forms of communication.[26]

It was a theory accessible to both the biologists who used it to explain the neurological messaging system, and the humanities academics.

Information Theory seeded these fields or gave them a "dramatic rethinking."[27]

> Weiner [a prominent information theoretician] told them all that these sciences, the social sciences especially, were fundamentally the study of communication, and that their unifying idea was the *message.* The meetings began with the unwieldy name of Conferences for Circular Causal and Feedback Mechanisms in Biological and Social Systems and then, in deference to Weiner, whose new fame they enjoyed, changed that to Conference on Cybernetics.

---

[24] *Ibid.,* 242.
[25] For negative interpretations of Information Theory see Solana-Ortega's "The Information Revolution is Yet to Come." Alberto Solana-Ortega, "The information revolution is yet to come (an homage to Claude E. Shannon)," (paper presented at the American Institute of Physics conference, Baltimore, Maryland, August 4-9, 2001) 465-466. http://eds.a.ebscohost.com/eds/pdfviewer/pdfviewer?sid=2cd4d7b2-692f-4ebf-84ca-09b271bce1f8%40sessionmgr4003&vid=0&hid=4103
[26] Warren Weaver, "Recent Contributions to the Mathematical Theory of Communication," in *The Mathematical Theory of Communication* (Chicago: University of Illinois Press, 1949): 14.
[27] Geoffrey Nunberg, "James Gleick's History of Information," *The New York Times,* March 18, 2011, *http*://www.nytimes.com/2011/03/20/books/review/book-review-the-information-by-james-gleick.html?pagewanted=all.

The following became so large that to address the new adherents Shannon wrote an essay literally titled "The Bandwagon."[28]

In it, Shannon said, "In the first place, workers in other fields should realize that the basic results of the subject are aimed in a very specific direction, a direction that is not necessarily relevant to such fields as psychology, economics, and other social sciences."[29]

Shannon pointed out a fundamental disconnect at this early stage, or perhaps prelude to, the Information Age. These academics did not grasp Shannon's fundamental point that "information" in his world was merely the transmission of neutral symbols, which at the time was inconsistent with the humanities and social sciences.

The conferences ended in 1953, only three years after they began.

> The Macy cyberneticians held their last meeting in 1953, at the Nassau Inn in Princeton…Given the task of summing up, McCulloch sounded wistful. 'Our consensus has never been unanimous,' he said. 'Even had it been so, I see no reason why God should have agreed with us.'[30]

Apart from infusing a more purely scientific perspective into the newfound social sciences, for Information Theory the conferences and bandwagon left behind not much more than an interesting historical anecdote.

> In the social sciences, the direct influence of information theorists had passed its peak. The specialized mathematics had less and less to contribute to psychology and more and more to computer science. [31]

The application of Information Theory continued most strongly inside mathematics and the sciences. Shannon's warning was heeded, either by choice or forcibly. The inter-disciplinary dialogue subsided. However, within the realm of pure science and

---

[28] Claude Shannon, "The Bandwagon," *IRE Transactions – Information Theory* (1956): 3, http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1056774.
[29] Shannon, "The Bandwagon," 3.
[30] Gleick, *The Information*, 263.
[31] *Ibid.,* 268.

engineering, technology was evolving towards applications which invited the first debate about cyber cryptography.

3.1 Analyzing the terms of Shannon's warning

In the 1950s, ARPANET, the predecessor of the Internet, had not yet come into being. A computer network did not exist, not even a domestic connection between two computers, coast to coast. The first time two computers directly communicated with each other was in 1965 between the TX-2 computer and Q-32 mainframe from Massachusetts to California.[32]

As such, Information Theory, mathematical at its core, was too young to handle the humanistic interpretations Shannon warned against. Information Theory's technologies had not yet been fully conceived, had not yet matured, let alone been deployed for mass use.

However, in the 21st century mobile technologies have pervaded our social and professional lives. Nearly two-thirds of Americans own smartphones.[33] In 2016 the global number of smartphone users exceeded 2 billion.[34] In 2015 a Heartland Monitor poll found that 44% of American mobile users primarily use their smartphone to access

[32] New Media Institute, "History of the Internet," accessed May 6, 2016, http://www.newmedia.org/history-of-the-internet.html.
[33] Aaron Smith, "U.S. Smartphone Use in 2015," Pew Research Center, April 1, 2015, http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.
[34] Statista, "Number of smartphone users worldwide from 2014 to 2019 (in millions)," 2016, http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/

the internet, and 9% use a tablet for this purpose.[35] Sixty-four percent of Americans own smartphones, and 7% rely heavily on their smartphones for online access. In many respects, America is now a smartphone-dependent population.[36]

The line between phone and computer has blurred. The related use of and access to information is now the front line of a profound policy discussion by stakeholders in this flow of information, called the "Crypto Wars".

In "The Bandwagon" Shannon said:

> Information theory has, in the last few years, become somewhat of a scientific bandwagon. Starting as a technical tool for the communication engineer, it has received an extraordinary amount of publicity in the popular as well as the scientific press. In part, this has been due to connections with such fashionable fields as computing machines, cybernetics, and automation; and in part, to the novelty of its subject matter. As a consequence, it has perhaps ballooned to an importance beyond its actual accomplishments. Our fellow scientists in many different fields, attracted by the fanfare and by the new avenues opened to scientific analysis, are using these ideas in their own problems. Applications are being made to biology, psychology, linguistics, fundamental physics, economics, the theory of organization, and many others. In short, information theory is currently partaking of a somewhat heady draught of general popularity.[37]

Two points to be made here: First, the importance of Information Theory has grown exponentially as an application of its resulting technologies. "…[A]n importance beyond its actual accomplishments" no longer applies. Information Theory's technologies are involved on the broadest social, political, cultural scales, and the minutia of our everyday lives. Second, the "connection to fashionable fields" and "their own problems" are incidental to Information Theory itself. We have now reached a point where Information Theory's technologies can now be applied and considered in a far broader sense.

[35] FTI Consulting, "Allstate/National Journal Heartland Monitor XXIV Key Findings," September 18, 2015, 2, http://heartlandmonitor.com/wp-content/uploads/2015/09/FTI-Allstate-NJ-Heartland-Poll-XXIV-Findings-Memo-Sept-24-2015.pdf
[36] Smith, "U.S. Smartphone Use in 2015."
[37] Shannon, "The Bandwagon," 3.

The Crypto Wars of the 1990s and 2010s, which dealt with the ethics of information technologies as they were progressively deployed in our society, provide a useful perspective on this renewal of meaning.

4. The Crypto Wars

Pulitzer Prize winning writer Joe Rago calls recent events like the FBI-Apple dispute the "encryption cold war."[38] This essay's comparison of the 1990s Crypto War and the 2016 debate over cryptography will make their similarities clear, but for simplicity's sake this essay will call the current debate the "2010s Crypto War" or the ongoing or current debate, and the 1990s Crypto War as simply that, or the first Crypto War.

4.0 The 1990s Crypto Wars

On February 4th 1994, "the White House announced its approval of the Clipper Chip, a device which would have protected private information but subject to an embedded method for governments to access the information in certain circumstances. The chip had been under study as a Government standard since April 1993. With the approval, and the first Crypto War broke out in full force."[39]

Later that year, in July 1994, AT&T Bell Laboratories researcher Matt Blaze found a serious flaw in the Clipper Chip technology.[40] "Yet," the *New York Times* reported in July, "the defenders of Clipper have refused to back down, claiming that the scheme – which is, they often note, voluntary – is an essential means of stemming an increasing threat to public safety and security by strong encryption in everyday use."

The first Crypto War also brought with it export restrictions on the strength of encryption that American companies could send abroad. Swire and Ahmad's review of the Crypto

[38] Joe Rago, "The White House should have avoided this legal and security showdown," *The Wall Street Journal,* February 19, 2016, http://www.wsj.com/articles/the-fbi-vs-apple-1455840721
[39] Steven Levy, "Battle of the Clipper Chip," *The New York Times,* June 12, 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all.
[40] Matt Blaze, "Protocol Failure in the Escrowed Encryption Standard," AT&T Bell Laboratories, August 20, 1994, http://www.crypto.com/papers/eesproto.pdf

War's export restrictions is lengthy, but given the complexity of the politics and technology, is worth including here:

> The precise elements of the U.S. encryption export regime shifted during the 1990s, with the Commerce, State, and other departments playing different and varying roles. By the mid-1990s, export of even moderately strong encryption required a license from the Department of Commerce. Companies that pushed the envelope on encryption export faced the risk of denial and the inability to sell their goods overseas. The government would also periodically issue broad regulations affecting the export of encryption. A 1996 regulation, for instance, stated: "The plan envisions a worldwide key management infrastructure with the use of key escrow and key recovery encryption items."
>
> The export control regime meant that major information technology companies were constantly engaged in difficult negotiations with the federal government, especially because products were evolving so rapidly during this period of intense Internet growth. Export limits were particularly burdensome for the many IT companies that conducted substantial business overseas. Those companies faced the difficult choice of either selling weak encryption products in all markets, or else establishing two tiers of products, one for the U.S. market and one for export abroad. Over time, the export rules also faced mounting criticism for their effect on U.S. sales; strong encryption products that were created outside of the United States were not subject to U.S. export control rules. A growing concern was thus that strong encryption was in fact being deployed outside of the U.S., but the export controls were preventing U.S. companies from meeting that demand.
>
> The stakes were raised even higher in 1997, when the House Intelligence Committee passed a bill, drafted in large part by the FBI, which would have imposed criminal penalties on the manufacturing or distribution of domestic encryption products that did not contain a government-mandated back door. Previously, the U.S. had permitted research and use of strong encryption within the country. Limiting the strength of domestic encryption, however, was a logical component of the FBI view that it should have the ability to decrypt communications that it lawfully received, including for U.S. communications. Limits on domestic encryption also were important to the FBI because of doubts about the effectiveness of export controls—software deployed in the U.S. would likely spread abroad over time, despite export rules. Proposed limits on domestic encryption, however, lifted the intensity of the crypto wars to a new level, directly affecting many users and researchers who were not involved in the export of commercial products."[41]

Swire and Ahmad's review details the chaos the encryption export restrictions brought before most of the restrictions were lifted in 1999, at which point the American encryption market opened up again. The Clipper Chip technology was dropped by the government at the same time. The simultaneous reversal signalled a sudden moderation in

[41] Peter Swire and Kenesa Ahmad, "Encryption and Globalization," *The Columbia Science & Technology Law Review* XIII (2012): 438-439, https://iapp.org/media/pdf/knowledge_center/Encryption_and_Globalization.pdf.

the government's encryption policy. The 1990 Crypto War was over but issues of personal security to information and third party access remained unresolved.

The lasting and landmark result from the first Crypto War is the Digital Telephony and Communications Privacy Improvement Act of 1994 (also known as the Communications Assistance for Law Enforcement Act, CALEA),[42] passed in October 1994 and put into effect in 1995,[43] which requires telecommunications carriers ("traditional telephone systems"[44]) to ensure wiretapping access in their infrastructure.

Although the omission was not considered relevant at the time it was adopted, and despite contrary arguments by the U.S. Department of Justice,[45] CALEA does not cover smartphones.[46] It also does not apply to the FBI-Apple dispute where Apple is not acting as a telecommunications carrier.[47]

4.1 The 2010s Crypto Wars

Following the 1990s Crypto War a conflict with the same competing interests at stake arose between the American government and several major American technology companies.

[42] "Ask CALEA, Communications Assistant for Law Enforcement Act," June 22, 2011, https://askcalea.fbi.gov.
[43] "6.095/STS095: Selected items on Digital Telephony Act," last modified October 19, 1997, http://groups.csail.mit.edu/mac/classes/6.805/articles/digital-telephony/digital-telephony.html
[44] Swire and Ahmad, "Encryption and Globalization," 432.
[45] Albert Gidari, "DOJ Misleads Court on the CALEA in the Apple Case," The Center for Internet and Society, Stanford Law School, March 11, 2016, http://cyberlaw.stanford.edu/blog/2016/03/doj-misleads-court-calea-apple-case
[46] Kristin Finklea, "Smartphone Data Encryption: A Renewed Boundary for Law Enforcement?", CRS Insights, October 17, 2014, https://www.fas.org/sgp/crs/misc/IN10166.pdf
[47] Albert Gidari, "CALEA Limits the All Writs Act and Protects the Security of Apple's Phones," February 19, 2016, The Center of Internet and Society, Stanford Law School, http://cyberlaw.stanford.edu/blog/2016/02/calea-limits-all-writs-act-and-protects-security-apples-phones

In February 2016, under the authority of the All Writs Act of 1789, which orders compliance with requests from courts of law, the FBI requested that Apple create new software (a "back door") to unlock the San Bernardino shooter's work-issued iPhone 5C. Apple handed over the cloud data stored from the San Bernardino shooter's iPhone.[48] But the iPhone hadn't been backed up for weeks, and the FBI wanted more recent, useful information. Apple could not break into the phone with its existing tools as their phones are designed for user's maximum data protection, even from Apple itself.

Applying its policy of user sovereignty as a tenet of design, Apple refused the FBI's request. If the FBI's request was applied to all iPhones and all companies like Apple, the result would be universal access for supposedly exceptional circumstances defined the government and its agencies. In certain respects, this was a replay of the Clipper chip controversy.

Before a scheduled hearing on March 22, 2016 the FBI obtained a delay, citing the availability of a third party able to break into the phone, and on March 28, 2016 withdrew its request, saying that the unnamed third party was successful. This left the conflict and underlying policy and philosophical issues between Apple and the FBI legally unresolved, a legal grey area applying to all tech companies that encrypt their data with similar methods.

Less than a month after the inconclusive FBI-Apple dispute, on April 13, 2016, American Senators Burr and Feinstein introduced draft legislation that requires all American companies' data to be "rendered intelligible," with limited exceptions, and requiring tech companies to use "key escrow" for all their encrypted data; essentially a "back door" for when law enforcement requests access to data under warrant. Key escrow constitutes a measure that fundamentally compromises the integrity of the mobile network, as the "back door" could be used by cybercriminals.

[48] Rago, "The White House should have avoided this legal and security showdown."

The terms of the intelligibility the Burr-Feinstein bill requires remain unclear, and the tech community, those who would be forced to practically implement the restrictions and act as compliance officers, is unwilling to comply.

Apple refuses to be co-opted by the government. As a manufacturer of information technologies Apple's refusal acts as a litmus test for the baseline evolution from the time of Shannon's warning, when information's meaning was secondary to its place in communications systems.

5. A Crypto Wars Comparison

5.0: A lot can happen in twenty years

Although the Crypto Wars are about different technologies (telecommunications in the 1990s and the iPhone in the 2010s), the American government's legal demand in each war is the same: exceptional access. The conceptual basis of the technology community's response is also the same in respect of both Crypto Wars: due to the flawed method of exceptional access, the technology used would present ethical problems bordering on human rights issues. This ethical problem has become clearer in the second Crypto War.

A more detailed comparative analysis of the two Crypto Wars will show why the common legal demand is important at this point in time to the moral and ideological escalation in the 2010s Crypto War.

The battlegrounds match: technologists against the American government; the government's attempt to impose a structural change on mobile communications systems (Clipper Chip in the 1990s, key escrow in 2016); and systemic change to the engineering of communications systems (Matt Blaze in the 1990s,[49] the testimony of dozens of computer experts in 2016[50]).

While the issue of exceptional access existed in both wars, there is a significant difference between the two: the 2010s Crypto War has no equivalent to the Clipper Chip of the 1990s Crypto War.

---

[49] Blaze, "Protocol Failure in the Escrowed Encryption Standard."
[50] Bruce Schneier, "Cyberweapons Have No Allegiance," February 25, 2015, https://www.schneier.com/essays/archives/2015/02/cyberweapons_have_no.html; John Markoff, Katie Benner, Brian X. Chen, "Apple Encryption Engineers, if Ordered to Unlock iPhone, Might Resist," *The New York Times,* March 17, 2016, http://www.nytimes.com/2016/03/18/technology/apple-encryption-engineers-if-ordered-to-unlock-iphone-might-resist.html?_r=1; Katie Benner and Nick Wingfield, "Apple is Rolling up Backers in iPhone Privacy Fight Against FBI," *The New York Times,* March 3, 2016, http://www.nytimes.com/2016/03/04/technology/apple-support-court-briefs-fbi.html?_r=0; Steven Murdoch, "Apple vs. FBI," University College London, April 20, 2016, https://www.ucl.ac.uk/news/headlines/0416/200416-apple-fbi;
Mike McConnell, Michael Chertoff, William Lynn, "Why the fear over ubiquitous data encryption is overblown," *Washington Post,* July 28, 2015, https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html .

The government has not offered any technology with which to access the requested data. Apple's current method of iOS encryption allows only the user access to their device's data. Similar to a key maker melting down his master key after giving the customer the only copy. To access the data Apple would have to create a completely new piece of software to break into the phone – which is exactly what the FBI wanted Apple to do. Its request is not to hand over technology or incorporate technology for access, but to create new technology for the FBI. This would set a highly demanding legal precedent on tech companies. Further, the 2016 Burr-Feinstein bill presents sweeping legal regulations, perhaps more broad than CALEA's, that would disallow Apple's current method of encryption.

The goal of both Crypto Wars from the government's side appears identical, namely, attaining exceptional access. The practicalities of this exceptional access have wildly different consequences for the second Crypto War. The end goal for the 2010s Crypto War is a purely legal bridging between Silicon Valley and the American government, where tech companies are responsible for individual enforcement of exceptional access. New mobile technologies where manufacturers can create a "black box" for their users, protecting user data even from themselves, have changed the governmental approach to exceptional access.

With the FBI's request and the Burr-Feinstein bill's more general requirement for exceptional access, Shannon's original theory of process neutrality for communications systems has now been completely reversed. His famous diagram would now show arrows for incursions at multiple points. The legal regulations for exceptional access would not only conclude the Crypto Wars, but perceived from Shannon's starting point would set the tone for the Information Age.

5.1: It's a smartphone world

As mentioned above, CALEA, a law requiring exceptional access for telecommunications, was enacted during the 1990s Crypto Wars.

FBI Director James Comey, a key player in the current debate, said in 2014 that:

> … the Communications Assistance for Law Enforcement Act, or CALEA, was enacted 20 years ago—a lifetime in the Internet age. And it doesn't cover new means of communication. Thousands of companies provide some form of communication service, and most are not required by statute to provide lawful intercept capabilities to law enforcement. What this means is that an order from a judge to monitor a suspect's communication may amount to nothing more than a piece of paper. Some companies fail to comply with the court order. Some can't comply, because they have not developed interception capabilities.[51]

In result, the Crypto Wars have changed to focus on mobile technologies. The FBI-Apple dispute, the goal of the Burr-Feinstein bill and the 2014 Riley v. California case, discussed below, all centre around smartphones and their lack of legal regulation.

As Rajamaki et al. say in "Building Trust between Citizens and Their Governments, A Concept for Transparent Surveillance of Suspects," "…telephone tapping under warrant does not provide police with the information it used to due to the technical developments of cellular telecom markets."[52]

"This is a data that was not available anywhere 10 years ago, it's a function of the smartphone," says Stephen Wicker, a Cornell professor of computer engineering

[51] James B. Comey, "Going dark," (speech delivered in Brookings Institution, Washington, D.C., October 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course

[52] Jyri Rajamaki, Juha Knuuttila, Harri Ruoslahti, Pasi Patama, Jouni Viitanen, "Building Trust between Citizens and Their Governments, A Concept for Transparent Surveillance of Suspects." European Intelligence and Security Informatics Conference (EISIC), 2015. http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/2_events/workshops/2015/20151208/Transparent%20surveillance%20of%20suspects%20for%20building%20trust%20between%20citizens%20and%20their%20governments.pdf

specializing in mobile computing security, about data now pursued by government agencies.[53]

The first Crypto War occurred two decades ago. While exceptional access as the main points of contention is the same, the form of end goals are new and the game has changed.

In fact, until very recently, "purpose-built evidence gathering technology," an offshoot of mobile forensics, was not used. In a culture of device and software generations, only purpose-built evidence gathering technology can compete with perpetually refreshed versions of operating systems and devices.

The government now relies on a collection of companies, whose tools are vetted by the National Institute of Justice, for newly invasive methods of mobile forensic extraction such as "exploiting existing vulnerabilities in the phone's software or introducing a forensic bootloader, a unique piece of the software that loads a version of the operating system to allow for the extraction of the device's file system."[54]

This was how the FBI cracked Apple's iPhone.[55] At the Aspen Security Forum in London, FBI Director James Comey gave an estimate of how much the bureau paid for an anonymous third party to unlock the iPhone: "A lot. More than I will make in the remainder of this job, which is seven years and four months for sure. But it was, in my view, worth it." News agencies immediately got to work calculating an estimation based on Comey's salary, coming up with an amount "That suggests the FBI paid the largest every publicized fee for a hacking job, easily surpassing the $1 million paid by U.S. information security company Zerodium to break into phones."[56]

---

[53] Rob Lever, "In Apple vs. FBI case, compromise appears elusive," *Phys Org,* March 6, 2016, http://phys.org/news/2016-03-apple-fbi-case-compromise-elusive.html

[54] Alex Hew, Damian Kumor, Rick Mislan, "Apple Has Already won. Now It Should Crack the San Bernardino iPhone," *IEEE Spectrum,* February 22, 2016, http://spectrum.ieee.org/view-from-the-valley/consumer-electronics/portable-devices/apple-has-already-won-now-it-should-crack-the-san-bernadino-iphone

[55] Juli Clover, "FBI Used Security Flaw Found by 'Professional Hackers' to Crack San Bernardino Shooter's iPhone," *MacRumors,* April 12, 2016, http://www.macrumors.com/2016/04/12/iphone-5c-flaw-fbi-professional-hackers/

[56] Julia Edwards, "FBI paid more than $1.3 million to break into San Bernardino iPhone," *Reuters,* April 22, 2016, http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB.

It should also be noted that in contrast to the Clinton administration, in office during the first Crypto War, the Obama administration has declined to support the Burr-Feinstein bill and has refused to comment on the FBI-Apple dispute. The White House has not taken a firm stance on encryption in contrast to the Clinton administration in the 1990s.[57]

However, in a recent interview at the 2016 South by Southwest Interactive (SXSW), President Obama expressed the necessity of legal exceptional access for law enforcement, but mediated by reason. "There are very real reasons why we want to make sure the government cannot just willy-nilly go into everyone's iPhones—smartphones—that are full of personal data."[58]

It seems that Obama, in the final months of his presidency, will only urge moderation for the debate instead of stepping into the fray. "I suspect the answer is going to come down to how do we create a system where encryption is as strong as possible; the key is secure as possible and is accessible by the smallest number of people possible."

Obama's stance is consciously moderate, "You can't take an absolutist stance on this…" but without action Obama leaves other political players in government surveillance to their own absolutism. FBI Director James Comey is an example.

In a 2014 speech Comey said that *now* is the time to incorporate changes, rather than later:

> …It makes more sense to address any security risks by developing intercept solution during the design phase, rather than resorting to a patchwork solution when law enforcement comes knocking after the fact. And with sophisticated encryption, there might be no solution, leaving the government at a dead end—all in the name of privacy and network security.[59]

---

[57] Jon Brodkin, "Report: 'Deeply divided' White House won't support anti-encryption legislation," Ars Technica, April 7, 2016, http://arstechnica.com/tech-policy/2016/04/white-house-reportedly-wont-support-anti-encryption-legislation/.
[58] Caitlin McGarry, "Obama on encryption: 'It's fetishizing our phones above every other value'", *Macworld,* March 11, 2016, http://www.macworld.com/article/3043553/security/obama-on-encryption-its-fetishizing-our-phones-above-every-other-value.html.
[59] Comey, "Going dark."

The Crypto Wars have flared again, this time with a more general legal orientation led by determined participants like Comey. The biggest difference between 1990 and 2016, smartphone technology, is necessitating the government's pursuit of legal means ahead of access itself.

The Internet Association, in a March press release, said that the Burr-Feinstein bill actually violates CALEA.[60] As any and all success from the first Crypto War is now impotent, the government is throwing their legal net as widely as possible to enforce exceptional access to smartphones and, learning from their mistakes, any technologies that might arise in the future.

The cryptography debate is being fought against the conceptual backdrop that information, however delivered, stored and accessed, is not just information. It is now the medium by which both lawful and unlawful activity is conducted. Government policy which was focussed on specific means under CALEA, telecommunications, is now focussed on information itself.

Information, and not just technology, is the 2010s Crypto War's focus, which is why Apple has drawn a line[61] between providing the government with user data and the government's requirement that it actively build the means for a back door into its technology. This is why the Burr-Fenstein legislation purports to require not just an obligation to turn over information but to provide technical assistance to obtain information. Number Five of Section Two states,

> …to uphold the rule of law and protect the interests and security of the United States, all persons receiving an authorized judicial order for information or data must provide, in a timely manner, responsive, intelligible information or data, or appropriate technical assistance to obtain such information or data…

[60] Internet Association, "Internet Association, CCIA, and i2Coalition Filed Amicus in Apple Case," press release, March 3, 2016, https://internetassociation.org/030316encryption/
[61] Apple, "A Message to our Customers," February 16, 2016, http://www.apple.com/customer-letter/.

Government policy and legal strategy is beginning to understand what Floridi already posits is the case for the Information Age.

Without a conscious appreciation of this reality, policy is likely to be inconsistent and incoherent. The Burr-Feinstein bill incorporates the scale of information technologies in its language, but not their complexity. From a technologist's perspective, the bill is a brute force and high-risk means of exceptional access. Let us consider attempts at compromise between competing interests in the current debate.

6. The straight math of "Keys under doormats"

"Keys under doormats," by Harold Abelson et. al is an essay written by over a dozen computer scientists who rejoined to write another paper after writing a similar security analysis in 1997 during the first Crypto Wars.[62] "Keys under doormats" explains what government agencies are actually asking for.

Before delving in it is important to note that before Whitfield Diffie and Martin Hellman published their paper "New Directions in Cryptography" in 1976, the American government held a monopoly on cryptography, through the National Security Agency (NSA) in particular.[63] Back then, establishing legal claim to exceptional access was not an issue.

Diffie and Hellman's paper described a split-key system where each user has a public and private key. This is also known as public key encryption. Sender and recipient strategically share these keys to send messages between each other only they can verify, using digital signatures for verification.

After "New Directions" was published the split-key system allowed for private and commercial cryptography beyond government control, and reliable privacy became a standard for private digital communications.

This shift initiated the government's desire for legal means of controlling encryption. "By the end of the George H.W. Bush administration in 1992, non-NSA encryption had become an important issue for national security policymakers."[64]

[62] Harold Abelson et al., "Keys under doormats: mandating insecurity by requiring government access to all data and communications," *Journal of Cybersecurity* (2015): 1-11, http://academiccommons.columbia.edu/catalog/ac:127127.
[63] Swire and Ahmad, "Encryption and Globalization," 433.
[64] *Ibid.,* 434.

Abelson et al. explain that the practical implementation of the exceptional access the American government is demanding is 'key escrow' aka a 'fair cryptosystem' where decrypt keys are held in escrow for authorized third parties.

However, it has been suggested that key escrow and the banning of forward secrecy would cause great damage to the integrity of communications systems.

Abelson et al. warn that,

> …An exceptional access requirement overlaid on the traditional content surveillance will put the security of the content at risk…" and, "To the extent that capabilities exist to provide law enforcement exceptional access, they can be abused by others.[65]

It is important to note that these are not commercial technology companies but individuals, computer scientists taking what they think is necessary action for scientific integrity. There is a considerable amount of materials available from a range of technologists on the practicalities of key escrow and how it compromises network security.

As Abelson et al. says, US and UK government proposals for,

> Data storage and communications systems…designed for *exceptional access* by law enforcement agencies…are unworkable in practice, raise enormous ethical and legal questions, and would undo progress on security at a time when Internet vulnerabilities are causing extreme economic harm.
>
> …The complexity of today's internet environment, with millions of apps and globally connected services, means that new law enforcement requirements are likely to introduce unanticipated, hard to detect security flaws. Beyond these and other technical vulnerabilities, the prospect of globally deployed exceptional access systems raises difficult problems about how such an environment would be governed and how to ensure that such systems would respect human rights and the rule of law.[66]

[65] Abelson et al., "Keys under doormats," 8.
[66] *Ibid.*

It should be noted that these authors, engineers and scientists, point out that this is both a social and ethical as well as technical debate. This aligns with the increasing ethical consequences of information technologies.

Participating via live stream in The Century Foundation's April 2016 debate called "National Security," Edward Snowden said,

> My opponent hopes that somebody could perhaps find a way for encryption to work only for the good guys. But encryption is a field of mathematics and no matter how much we might hope otherwise, math is math. It works the same for Mother Theresa as it does for Osama Bin Laden.[67]

[67] Debates of the Century, "National Security", April 26, 2016, YouTube video, uploaded May 1, 2016, https://www.youtube.com/watch?v=-yoyX6sNEqs.

7. Clap if you believe in absolute security

In contrast to the above explanation of the "pro-cryptography" side of the debate, the opposite stance advocates exceptional access even with the above testimony from industry experts. This side is not as much "anti-cryptography" as it is "pro-law."

Snowden's opponent in the 2016 debate, Fareed Zakaria, an American journalist and author, said that we cannot have a field of absolute privacy, a black box. Zakaria clarified he is not anti-cryptography, only pro-rule-of-law, with all the consequences of that alignment. Zakaria is against,

> A 'zone of immunity' in which no laws can reach, no courts can reach, no government can reach…the case is very simple, which is, are we a society of laws? Is there some process of law by which a government, a democratically elected government with independent courts has the authority to access information? …I understand that within a democracy if you have rules of law, you have to sacrifice liberty for security at some point. This is not an absolutist position, I believe in strong protections for those liberties, I do not believe in the government abusing its authorities, I believe it has, but you cannot have an absolute zone of privacy.
>
> …You cannot have liberty in the absence of law. That is the jungle…if you want to live in a democratic society that has rules, the authorities have to have some recourse to lawful court orders.[68]

To conclude, Zakaria cited the 1974 unanimous ruling in the United States vs. Nixon,

> The Supreme Court ruled…'no person, not even the President of the United States, is completely above the law, and the president cannot use executive privilege as an excuse to withhold evidence that is demonstrably relevant in a criminal trial.' That is the issue. No one in America can withhold evidence that is relevant to a court. Not the president, not the world's most powerful company, not an individual, not even the most shiny and alluring product, not even an iPhone, is above the law.

Zakaria literally states that at its core the case is about whether America is "a society of laws." After Zakaria spoke, in his opening statement Snowden said,

[68] Debates of the Century, "National Security."

> Let's start with what tonight is not about. Fundamentally, tonight is not about politics. Nor is it really about the law. It's about science. For that reason it doesn't really matter whether you're for or against surveillance. Because by the end of this debate we'll have established that the proposition is not really a choice between privacy and security. It's rather about more security or less security.

In striking contrast, Snowden rejected the premise of Zakaria's position altogether. These are the kinds of "absolutist stances" President Obama is wary of.[69]

Yet the opening of the Burr-Feinstein bill casts a vast legal net and requires, as shown above, the active participation of technology companies in designing, or assisting in the design, of back-door entry into personal information.

The Burr-Feinstein bill reminds us that Silicon Valley is still in America.

Citing Snowden to elucidate the Silicon Valley side of the debate may seem a biased choice. But it is acceptable given that Snowden is siding, as he says "standing shoulder to shoulder", with the Director of the NSA on this issue; astounding given the basis of his reputation, the classified information he leaked from the NSA in 2013.[70] A paradigm shift is redrawing former political boundaries.

Still, the "National Security" debate truly exemplifies the polarity of the issue at hand. Zakaria and Snowden couldn't agree on what the "National Security" debate was really about, politics or mathematics. Of course, it is both.

Apple's political position creates a technological black box, an absolute zone of immunity for its users. The black box may exist because of straight math as Snowden says, but is automatically and unavoidably politicized.

---

[69] McGarry, "Obama on encryption."
[70] Rebecca Savransky, "Snowden: Without encryption, everything stops," *The Hill,* May 1, 2016, http://thehill.com/blogs/blog-briefing-room/news/278320-snowden-without-encryption-everything-stops

The black box both represents and manifests a lawless zone, a flouting not only of the practiced laws of a democratically elected government, but the premise of that government's power to enforce those laws. Here, the limits to the government's rule of law are decided by an unelected, non-representative body. This is why the government is reaching back in time to the All Writs Act of 1789,[71] why the Burr-Feinstein bill describes reasons for legal compliance in such broad language, why *history holds importance in this debate.*

In the twenty years since the original Crypto Wars a middle ground has failed to manifest between technologists and politicians. Of course this is also due to the limits of our technology, as Abelson et al. detail above.

With such polarity that neither the straight facts of mathematics nor rule of law are able to bridge, there is no way forward. Standing still may result in moving backwards, as shown by Brazil's recent banning of Whatsapp for Facebook's failure to hand over documents for an ongoing criminal investigation (the same premise as the FBI-Apple dispute, although in a different political system);[72] as well as the FBI's failure to give Apple the information on the flaw they exploited to unlock the iPhone, which puts millions of Apple user's iPhone data at risk.[73]

[71] Eric Limer, "Most Useful Podcast Ever: Why is the FBI Using a 227-Year-Old Law Against Apple?", *Popular Mechanics,* February 24, 2016, http://www.popularmechanics.com/technology/a19483/what-is-the-all-writs-act-of-1789-the-225-year-old-law-the-fbi-is-using-on-apple/

[72] BBC, "WhatsApp Brazil: Judge lifts suspension of messaging service," May 3, 2016, http://www.bbc.com/news/world-latin-america-36199489

[73] Danny Yadron, "FBI confirms it wont' tell Apple how it hacked San Bernardino shooter's iPhone," April 28, 2016, https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino

8. A Sullied Silicon Neutrality

8.0 Silicon Valley, Washington

Now the difficulty will be in how to take this recognition, that communication systems and social engineering are one in the same, and create a balanced technology that optimizes security and limits legal exceptional access on a principled basis. One that effectively concludes the Crypto Wars.

The balance should not reflect the neutral nature of technology and should not manifest the nature of partisan politics. It should manifest the neutrality that both Information Theory and the law are supposed to work in practice.

This is no easy feat – the variegation of technology's application in different societies (think China's restrictions on using servers outside the mainland[74]) shows that technology very easily becomes its politics.

The socialization of technology, its unavoidable integration into a comparably complex and clouded social, political, cultural realm shows that in application, technology cannot be neutral.

Melvin Kranzberg puts it succinctly in his set of laws about technology, "Kranzberg's Laws," the first of which says that technology is "neither good nor bad; nor is it neutral."[75] Technology is what its application makes it.

However, as we have discussed, it would be short-sighted, given our dependence on information, to see the issues as merely about technology. The assumed distinctions between cars and mechanics, between cooks and diners, don't apply as neatly here. In

[74] David Barboze and Paul Mozur, "New Chinese Rules on Foreign Firms' Online Content," *The New York Times,* February 19, 2016, http://www.nytimes.com/2016/02/20/business/media/new-chinese-rules-on-foreign-firms-online-content.html?_r=0

[75] Melvin Kranzberg, "Technology and History: 'Kranzberg's Laws'", *Technology and Culture* 27 (1986): 545.

The Fourth Revolution Floridi says, "What I stress in this book is that sometimes it is a new millennium, and you are in the infosphere." And sometimes in the millenium's infosphere you are a computer scientist, sometimes a politician, sometimes in China, sometimes in North America – the nature of technology depends on the "sometimes."[76]

Silicon Valley's tech giants, such as Apple and its allies in the FBI dispute, show how democratizing communications technology can be, in their corporate culture and efforts to expand Internet access to the 60% of the world that has no access (Google's Project Loon, Facebook's Free Basics).[77] Such ubiquitous expansion of the internet aligns on the surface with Shannon's original credo for purely technological improvement, but since content is now meaningful, misaligns with the ideological shades of grey everywhere, even in the united front Silicon Valley's giants represent in the Crypto Wars.

Facebook's Free Basics has been criticized as disguised efforts to expand Facebook's reach instead of empowering the underprivileged with technology.[78] Facebook has also been accused of political bias in filtering conservative news articles from its supposedly algorithmically unbiased Trending Topics column.[79]

Microsoft's Bill Gates, one of the most influential tech leader in Silicon Valley, has sided with the American government over data access.[80]

Google faces multiple competition and antitrust rows,[81] and collects and sells its user's data while 65% of Americans mistakenly think a "privacy policy" means their data isn't shared with other websites or companies.[82] A now famous University of Pennsylvania

---

[76] Floridi, *The Fourth Revolution*, vii.
[77] Internet Live Stats, "Internet Users," http://www.internetlivestats.com/internet-users/ .
[78] Catherine Shu, "Facebook 's Save Free Basics in India" Campaign Provokes Controversy," *Tech Crunch,* December 17, 2015, http://techcrunch.com/2015/12/17/save-free-basics/ .
[79] Dave Lee, "Facebook: Political bias claim 'untrue,'" *BBC,* May 10, 2016, http://www.bbc.com/news/technology-36254201.
[80] Matt Burgess, "Bill Gates backs FBI in Apple's iPhone encryption battle," *Wired,* February 23, 2016, http://www.wired.co.uk/news/archive/2016-02/23/bill-gates-support-fbi-apple .
[81] Huffington Post, "Google Antitrust," http://www.huffingtonpost.com/news/google-antitrust/ .
[82] Nora Draper, Michael Hennessy, Joseph Turow, "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation," New Annenberg School of Communication, University of Pennsylvania, June 2015, https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and.

study released in June 2015 shows that a majority of Americans are "resigned to giving up their data—and that is why many appear to be engaging in tradeoffs" with companies such as Google for services.[83]

And unavoidably, Apple's position against the FBI is also a marketing stance that creates a niche for itself in the mobile devices market.[84]

Therefore the political tug-of-war for neutrality between technology and the law is also an argument over righteous neutrality. In the 2010s Crypto War both sides contain an ideological core for human rights. What is more important to human rights: security or privacy? It is an impossible contest between similarly moral concerns.

In the Crypto Wars no one truly represents Shannon's purist technological stance, both because the social context has changed, and because the mouthpieces of both sides of the current debate are integrated into this social context. This includes the governmental side.

The Burr-Feinstein bill is still a discussion draft. It has been given "poor odds" of passing, has been condemned by members of Congress, including Senator Wyden who says he will filibuster the bill,[85] and the White House has "refused to endorse it". [86]

The bill is contrasted by a more lenient, comprehensive option, [87] the McCaul-Warner Commission.[88]

---

[83] Draper, Hennessy, Turow, "The Tradeoff Fallacy," 3, 9.
[84] "For Apple, security is also a global marketing strategy. New security measures would not only help the company in its fight with the government, but also reassure investors and customers." Matt Apuzzo and Katie Benner, "Apple Is Said to Be Trying to Make It Harder to Hack iPhones," *The New York Times,* February 24, 2016, http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html?smid=fb-nytimes&smtyp=cur&_r=1&mtrref=undefined.
[85] Kate Conger, "Burr-Feinstein encryption bill is officially here in all its scary glory," *Tech Crunch*, April 13, 2016, http://techcrunch.com/2016/04/13/burr-feinstein-encryption-bill-is-officially-here-in-all-its-scary-glory/
[86] Riana Pfefferkorn, "The Burr-Feinstein Crypto Bill Would Gut Our Cybersecurity," The Center for Internet and Society, Stanford Law School, April 26, 2016, http://cyberlaw.stanford.edu/publications/burr-feinstein-crypto-bill-would-gut-our-cybersecurity.
[87] Ryan Hagemann and Andrew Chang, "Encryption showdown: Burr-Feinstein vs. McCaul-Warner," *The Hill,* April 25, 2016, http://thehill.com/blogs/congress-blog/technology/277467-encryption-showdown-burr-feinstein-vs-mccaul-warner.

A similar anti-cryptography bill, Assembly Bill 1681[89] that would have authorized "$2,500 penalties against phone manufacturers and operating system providers if they do not obey court orders to decrypt phones", was defeated in April 2016.[90]

Finally, many technologists believe the FBI is wilfully weakening encryption for its own political gain, instead of valid legal requirements. They "contend the FBI's approach to encryption weakens data security for many smartphone and computer owners in order to preserve options for federal investigators to open locked devices."[91]

8.1 A sticky end to Lollipop

History tells us to be mindful of applied neutrality, which is never neutral. The ideology accompany the "straight math" of Silicon Valley's side of the debate is sullied by the means of asserting itself. The encryption Apple uses on its mobile operating system was not an organic evolution of their technology but a timed political statement.

Within the same month (September 2014) that Apple announced iOS 8 would include stronger encryption that bars access to the device everyone but the user from the device,

---

[88] McCaul-Warner Commission on Digital Security, https://homeland.house.gov/wp-content/uploads/2016/02/McCaul-Warner-Commission-One-pager-1.pdf.
[89] Andrew Crocker, "Worried about Apple? California Has a Bill That Would Disable Encryption on All Phones," Electronic Frontier Foundation, March 9, 2016, https://www.eff.org/deeplinks/2016/03/worried-about-apple-california-has-bill-would-disable-encryption-all-phones.
[90] Kevin Townsend, "California Quietly Drops Bill Requiring Phone Decryption," *Security Week*, April 15, 2016, http://www.securityweek.com/california-quietly-drops-bill-requiring-phone-decryption.
[91] Devlin Barrett, "FBI Plans to Keep Apple iPhone-Hacking Method Secret," *Wall Street Journal,* April 26, 2016, http://www.wsj.com/articles/fbi-plans-to-keep-apple-iphone-hacking-method-secret-sources-say-1461694735.

even Apple itself, Google announced its Android mobile operating system would also use such encryption.[92]

Prior to adopting iOS 8, user data was still accessible to Apple without having to construct a back door. After adopting iOS 8, only the PIN or passcode set by the iPhone's user could unlock the iPhone.[93] The technology for this level of encryption existed before iOS 8. It was Apple that decided when to implement the technology. The subject of the FBI-Apple dispute, the San Bernardino shooter's iPhone, uses iOS 9.[94]

Because Google does not manufacture hardware for their Android operating system its adoption of kinds of encrypted software is more complex. In late 2014 Google released Android 5.0 Lollipop with the default encryption setting already on. There were some hiccups with full encryption by default on Lollipop due to "performance issues."[95] But Android 6.0 Marshmallow, released in October 2015, required manufacturers to set encryption "on all devices out of the box." And it is clear that Android 6.0 Marshmallow carries the same premise as Apple's iOS 8 and later, encryption for all devices, the data inaccessible to anyone except the user.

As the FBI's Manhattan District Attorney's Office says in their November 2015 report "On Smartphone Encryption and Public Safety,"

> "Even before Apple's and Google's announcements, many devices had given users the option of enabling such powerful encryption. The significance of the companies' change in practice was that this type of encryption would be the default setting on their new devices."[96]

---

[92] AFP, "Google to Boost Android Encryption, Joining Apple," *Security Week*, September 18, 2014, http://www.securityweek.com/google-boost-android-encryption-joining-apple.
[93] Cyrus Farivar, "Apple expands data encryption under iOS 8, making handover to cops moot," *Ars Technica*, September 18, 2014, http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/.
[94] Cyrus Farivar "Judge: Apple must help FBI unlock San Bernardino shooter's iPhone," *Ars Technica,* February 17, 2016, http://arstechnica.com/tech-policy/2016/02/judge-apple-must-help-fbi-unlock-san-bernardino-shooters-iphone/.
[95] Lisa Vaas, "Google quietly drops promised encryption by default for Android Lollipop," *Naked Security*, March 4, 2015, https://nakedsecurity.sophos.com/2015/03/04/google-quietly-drops-promised-encryption-by-default-for-android-lollipop/.
[96] Manhattan District Attorney's Office, "On Smartphone Encryption and Public Safety," November 2015, http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

Neutrality is what Shannon desired for communications systems, what Silicon Valley advocates for protection of user data, and how the law is applied in a democracy. Yet it is scarce absolute in the Crypto Wars.

Silicon Valley and Washington may not act as straightforwardly moral as their arguments in the Crypto Wars, but the point is that their misaligned actions and creeds are part of the search for compatibility and understanding of the Information Age.

This essay's review shows a highly polarized debate about a technology that began as a simple and neutral conveyor of information. The laws, scandals and disputes since have shown no guiding principle or policy consciousness which could align their resolution with the nature of the changes this technology has created. So, what are the fundamental determinants of the debate? What is the nature of the fundamental shift informing, however cloudy, these limited nuances?

9. The Informational Paradigm Shift

9.0 History and the Information Age

A conscious appraisal of the role that information has come to play in our society should be discussed overtly if policy is to ultimately align itself with the reality of our dependence on that information. Luciano Floridi, in his book *The Fourth Revolution, How the Infosphere is Reshaping Human Reality,* defines an informational society as one dependent on information and communication technologies (ICTs). Our Information Age,

> …became a reality only recently, once the *recording* and *transmitting* facilities of ICTs evolved into *processing* capabilities. The profound and widespread transformations brought about by ICTs have caused a huge conceptual deficit.[97]

A "conceptual deficit" like the chasm between Silicon Valley and the American government in the current debate. The conceptual deficit is the no man's land, the unbridged absolutist ideologies, in the Crytpo Wars. Floridi goes on to say that a new mode of thinking, a new philosophy, is needed to fill the conceptual deficit to allow society to grapple with its new age.

> Given the unprecedented novelties that the dawn of the information era is producing, it is not surprising that many of our fundamental philosophical views, so entrenched in history and above all in the industrial age, may need to be upgraded and complemented, if not entirely replaced."[98]

This is the paradigm shift for which recognition is needed.

Floridi further explains:

> …only very recently has human progress and welfare begun to be not just *related to,* but *mostly dependent on*, the successful and efficient management of the life cycle of information.

[97] Floridi, *The Fourth Revolution*, ix.
[98] *Ibid.,* viii.

Floridi describes any society dependent on information as "hyperhistorical" , and that "Only a society that lives hyperhistorically can be threatened informationally, by a cyber attack."[99]

This last statement rings true in the ongoing debate, which was inflamed by the American government's request for a terrorist's data (the San Bernardino shooter). Floridi says,

> "It seems clear that a new philosophy of history…invites the development of a new philosophy of nature, a new philosophical anthropology, a synthetic environmentalism as a bridge between us and the world, and a new philosophy of politics among us."[100]

Shannon's warning came at a time before content and meaning became central to the transmission of information, and before the relevance of a philosophy of politics could be envisioned. Floridi proposes using philosophy to fill the conceptual deficit that has developed since, but the deficit must first be recognized with coherent policy to follow.

An alternative way to see the Information Age's paradigm shift and resulting "conceptual deficit" is through traditional information studies. Borgman distinguishes between an infrastructure *of* information and an infrastructure *for* information. Infrastructure *of* information is designed for ubiquitous usability, "the emphasis is on building a framework to support any kind of content; the meaning is in the eyes of the sender and the receiver."[101] Meaning is subordinated to utility.

Infrastructure *for* information considers the social relationship of the infrastructure. It is "by no means rational, objective…" An infrastructure *for* information is more consciously social, its design considers its relationship with its users.

Shannon's base unit of information, the ability to quantify it as a unit of measurement, is part of an infrastructure *of* information. Information's quantification is, and will always

---

[99] *Ibid.,* 3-4.
[100] Floridi, *The Fourth Revolution,* viii.
[101] Christine L. Borgman, *Scholarship in the Digital Age: Information, Infrastructure, and the Internet* (Massachusetts: MIT Press, 2007), 42.

be, an integral part to the Internet's engineering. But the same status for its framework, the "pipes of ice," is up for debate.

The paradigm shift is more than the previous shift from "script to print."[102] A shift to information technologies is a shift to a medium that channels itself. It is all enveloping, defining a new paradigm in new ways. Elizabeth Eisenstein, one of the first to point out the importance of the shift from script to print, "…believed that scholars were too often blinded to the effects of the very medium in which they swam."[103] With great vision, Eisenstein attributed Marshall McLuhan for "refocusing their gaze." [104] Our pipes of ice take McLuhan's credo even further. The medium literally is the message, and vice versa.

The Information Age will shift our infrastructure *of* information towards one *for* information. The solution for the "conceptual deficit" Floridi describes lies in this realization.

Such a paradigmatic shift, like script to print, has never occurred with history so easily available to us.[105] Why is there no historical lesson that can directly and instantly instruct our conflict between law and information technologies? Why, with history more available to us than ever through information technologies, can we not use that history to shape the Information Age?

Floridi defines the Information Age as "hyperhistorical," a completely new era, a new kind, of history defined by dependence on ICTs.[106] There is nothing beforehand with which to contextualize it. We can learn from history, but will not find a "quick fix", even in related events like Information Theory's founding. Like a black hole, the "conceptual deficit" is only visible by the distortion of matter around it. For this reason fundamental policy disputes like the Crypto wars are useful in outlining the matter.

---

[102] Gleick, The Information, 399.
[103] *Ibid.,* 399-400.
[104] *Ibid.,* 400.
[105] *Ibid.,* 400-401.
[106] Floridi, *The Fourth Revolution:* 3.

Similarly, in "The Information Age and the Printing Press," James Dewar posits that historical parallels are upset by the strength of networked computers as new technologies.[107] The comparison between Crypto Wars, between the polarities of the debate (Zakaria vs. Snowden), elucidate this deficit as a chasm between old modes of thinking and a gradual but imperfect realization of the new information dependent reality.

9.1 Claude and the Chasm

Floridi's definition of information is wildly different from Shannon's, or Gleick's. They may share a name, but represent different units of the same medium. Shannon's unit of information is purely statistical, quantified. Floridi's is social, and gives rise to philosophy.

Let us return to Chapter One's question and take Shannon's warning to its conclusion in the Crypto Wars. What would Shannon have said about the Crypto Wars? What would his chosen position be in the ongoing debate? Shannon likely would have sided with Apple and its allies. If Shannon warned that optimal engineering must take precedence over any non-scientific interpretation, we must assume that he would side against the compromising of the iPhone's security. Leave the engineering to the engineers.

Shannon's warning is not an active ethical tool. But in an ethical debate about technology Shannon's utilitarian approach picks his side for him. Like Snowden, Shannon didn't need to take sides, to say that the Kantian interpretation of Information Theory is more correct than the Nietzschian. For Shannon, Information Theory is not about interpretation at all but application, the engineering, the science, the technology.

[107] James A. Dewar, "The Information Age and the Printing Press, Looking Backward to See Ahead," the Rand Corporation, 1998, http://www.rand.org/pubs/papers/P8014/index2.html

But given the paradigmatic difference between Shannon's time and our own, is this really a logical, sustainable position? A true continuation of Information Theory's core, which is ultimately practical?

Shannon's original draining of meaning from communications systems was to quantify information for mathematical application. In fact, it was not the communication system that Information Theory drained of meaning. It was information itself, for the purpose of optimizing the communication system.

He made no claim on the nature of technology itself. He only claimed political, cultural, or social interpretation of technology to be subordinate to the practicalities of that technology. Shannon's mathematics and semantics were about the reality of engineering and the message – the *effective* building of Information Theory's technologies and how to practically use them.

The extent of communication technology's integration into our society has made meaning inextricable not with the message, but with the engineering systems that channel that message. Societal infrastructure must be able to "plug in" to communications systems as its citizens do.

In the paradigm shift of the Information Age, the distinction between engineering decisions and political decisions has eroded. This is not an adjustment of information's base unit, Shannon's definition of information, for technology. It would be presumptuous to put words into Shannon's mouth, but it is interesting and useful to speculate on his position in the Crypto Wars. The difference between our dependence on technology in Shannon's time and our current dependence throws our relationship with technology into greater relief. As James Gleick put it 2011 at a talk at Google's Mountain View, California office, "I believe that Shannon's theory, Shannon's and then all of the work that followed it by mathematicians and then soon after, computer scientists, lie

underneath the structure of our world, not just as a technical foundation, but in a more genuine way."[108]

With the scale and complexity communication technologies have reached in society, one is dependent on the other. The problem with the Information Age's co-dependent politics and technology is that as shown by the Snowden-Zakaria debate, neither sphere recognizes this in their fundamental ideologies. A viable dialogue must be able to take place for the sake of technological progress. Snowden and Zakaria must be able to concede they are debating the same issue.

Even if Gleick's interpretation of Information Theory's as a more "genuine" foundation is an overstatement, the origins of Information Theory at the beginning of the Information Age allow it to act as a point of reference. Every technology has a history. Most if not all technologies have been underutilized, misused, abused for political gain. Information Theory's technologies are no different. What is different is the extent to which they have changed in fifty years, and how those changes define our current politics.

Ultimately, there is more of a conceptual than technological continuation between the Crypto Wars. That is, increasing reliance on technology and increasing pressure from government to politically "plug in" to that technology.

And that increasing reliance is in large part due to the recent blurring of the line between phones and computers. The FBI-Apple dispute is over smartphone data, which constitutes a new kind of data previously, largely unharvested as a means of general surveillance by law enforcement. As Cornell computer engineering professor Stephen Wicker describes, "This is a data that was not available anywhere 10 years ago, it's a function of the smartphone."[109] Records of conversations, instant messaging, constantly updated from our pocket, are a new level of digital intimacy.

---

[108] James Gleick, "The Information: A History, a Theory, a Flood | Talks at Google," March 17, 2011, YouTube video, uploaded March 24, 2011, https://www.youtube.com/watch?v=iyOzSzcDwg8.
[109] Rob Lever, "In Apple vs. FBI case, compromise appears elusive," *Phys Org,* March 6, 2016, http://phys.org/news/2016-03-apple-fbi-case-compromise-elusive.html

9.2 Stepping into the chasm

64% of Americans own smartphones, and 7% rely heavily on their smartphone for online access. America is a "smartphone-dependent" population for which the 2014 Riley v. California case meant a great deal.[110] The Riley v. California case ruled that a warrantless cell phone search violates the Fourth Amendment right to privacy.

Comey's perspective claims to be neutral towards technology and this is precisely the kind of fundamental insensitivity to the paradigm shift that results in solutions that are not calibrated to the problem.

A common analogy used is: searching a phone is the same as searching a house. This is a digital interpretation of the Fourth Amendment, which says, "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures"[111] in the absence of a warrant.[112]

But as technologists like Tech Dirt's Tim Cushing points out, records of your conversations with your children, your spouse, your private thoughts, are not kept in your house.[113]

However, Chief Justice Roberts, who delivered the opinion on the Riley case, correctly perceived key aspects of the paradigm shift when he said, comparing the old way of searching someone's person to searching their phone is, "like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together." Analogies between personal spaces or items are not necessarily actionable connections.

---

[110] Aaron Smith, "U.S. Smartphone Use in 2015," Pew Research Center, April 1, 2015, http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.
[111] The Constitution of the United States, The Fourth Amendment.
[112] Amy Davidson, "Four Ways the Riley Ruling Matters for the N.S.A.", *The New Yorker,* June 29, 2014, http://www.newyorker.com/news/amy-davidson/four-ways-the-riley-ruling-matters-for-the-n-s-a
[113] Tim Cushing, "Comparing Cell Phones To Houses Not Exactly Deterring Use of Generalized Warrants, Court Finds," *Tech Dirt*, January 20, 2016, https://www.techdirt.com/articles/20160116/14332433358/comparing-cell-phones-to-houses-not-exactly-deterring-use-generalized-warrants-court-finds.shtml

The Riley v. California ruling exemplifies the reaction to mobile technologies, the paradigmatic shift towards the Information Age and the filling of its conceptual deficit. The analogies and language of old modes of thinking do not apply to the Information Age.

This is further reflected in Chief Justice Roberts consideration of the term "cell phone" as a misleading shorthand.

> Many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.[114]

This is a good example of the problem of the "gradual realization" of how vital both information and information delivery is to our modern existence. Chief Justice Roberts grasped the disconnect between our old mindset and what technology necessarily and intrusively provides.

The Riley v. California case touches "on questions of language and technology, and the way one shapes the other." Such as how "a phone is not a phone," as *New Yorker* Senior Editor Amy Davidson, who specializes in national security, puts it in her cover of the Riley v. California case.[115] How better to illustrate a paradigm shift than the sentence, "a phone is not a phone."?

[114] Supreme Court of the United States, *Syllabus*, Riley v. California, October 17, 2013, http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf
[115] Amy Davidson, "Four Ways the Riley Ruling Matters for the N.S.A.", *The New Yorker,* June 29, 2014, http://www.newyorker.com/news/amy-davidson/four-ways-the-riley-ruling-matters-for-the-n-s-a

10. Conclusion

We are now in a hyperhistorical era, defined more by our technology than by our past. Waking up to the extent and nature of our dependence also means waking to how it came about.

The second Crypto War was not a mere extension or escalation of the first. The second Crypto War concerned a new technology, smartphones, which confounds previous methods of accessing data. The conceptual continuation between the two Crypto Wars is a further evolution away from Shannon's purely technological perspective towards greater socio-political implications.

Floridi has been hired by Google to advise on the ethics of information. In his January 2016 talk at Trinity College Dublin Floridi said that Google hiring a philosopher is a bit like going to the dentist – you only force yourself to do so when absolutely necessary. Native to an era of comparatively severe social and technological segregation, a discussion of Information Theory in the context of the Crypto Wars may be like pulling teeth from an unwilling field, but one that is ripe for historical extraction.

As the US Department of Justice said in the FBI-Apple dispute, "technology, rather than the law" controls access to data. Such technology is like Floridi's pipes of ice channelling water. It is a subtle difference, but as the study of Shannon and the Crypto Wars shows, an important one for understanding the nature of its social integration.[116] The Crypto Wars are about technological accessibility, both physical and conceptual.

Before Diffie and Hellman's 1976 paper, the National Security Agency had direct control over the most sophisticated, therefore most secure, encryption,[117] and "By the end of the

[116] United States District Court for the Central District of California, "Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search," February 19, 2016, http://www.wired.com/wp-content/uploads/2016/02/Apple-iPhone-access-MOTION-TO-COMPEL.pdf
[117] Swire and Ahmad, "Encryption and Globalization," 433.

George H.W. Bush administration in 1992, non-NSA encryption had become an important issue for national security policymakers."[118]

Still, after 1976 means of access to data were within the government's potential reach. Though the Clipper Chip was flawed, it conceivably still could have been implemented by telecommunications companies without significantly altering network design, or them having to create new technology.

Then smartphones were introduced (the first iPhone came out in 2007[119]), "devices" constituted by both hardware and software, along with a sudden culture of new models, new releases of both hardware and software, software updates, push notifications, "synching" devices, and the Internet of Things. Technological culture rushed ahead of legal infrastructure. When phones became more than phones, phone companies became more than phone companies. They are present in their user's devices.

And after Apple adopted iOS 8 in 2014, no one, not even Apple itself, can access their user data. Government access necessitates not only physical changes to Apple's mobile network (its operating software), but by legal precedent changes user's rights and the concomitant culture of use.

A confrontation is being forced by this disordered evolution. A helpful metaphor for our current state is Floridi's rendition of a metaphor from Viennese philosopher Otto Neurath, "We do not even have a raft but drowning in obscurities is not an option…" Floridi's version is: "We need to make a rational effort and built a raft *while still swimming*. [emphasis added]"[120]

At this time the polarity of the Crypto Wars may only be resolved, if that is an acceptable term for ending legal recourse like the FBI-Apple dispute, by a serious reversal of current

[118] *Ibid.,* 434.
[119] "Years of the iPhone: An Interactive Timeline," *Time,* June 27, 2014, http://time.com/2934526/apple-iphone-timeline/
[120] Floridi, *The Fourth Revolution*, x.

trends on legislation for exceptional access. If we take Abelson et al. and the dozens of technologists at their word, a technology that allows both security and reasonable exceptional access is not in sight. Therefore what form this resolution will manifest is unclear. Simply agreeing upon the scope of the problem is difficult for industry experts, like the authors of the February 2016 Harvard study "Don't Panic, Making Progress on the 'Going Dark' Debate," concede.[121]

Nevertheless, with cases like Riley vs. California we are beginning to perceive, as Eisenstein put it, "the medium in which [we] swim." We are beginning to build a sustainable paradigm for the Information Age, and like Floridi's raft, we are constructing it "while swimming."

The first application of Shannon's technology was for the Space Race,[122] mankind's first step beyond any of his pre-existing domains: a lofty scientific and political race for a new age, in an arena only accessible conceptually, made real to the rest of the world through television screens.

Floridi asks where the increasing computing power of Moore's Law is devoted. "It is not that we are regularly putting people on the Moon with our smartphones and tables. The answer is: interactions, both machine-to-machine and human-computer ones, also known as HCI." That first application of Information Theory towards the Space Race has passed. The age of information has truly arrived.

[121] Urs Gasser, Nancy Gertner, Jack Goldsmith, Susan Landau, Joseph Nye, David R. O'Brien, Matthew G. Olsen, Daphna Renan, Julian Sanchez, Bruce Schneier, Larry Schwartztol, Jonathan Zittrain, "Don't Panic, Making Progress on the 'Going Dark' Debate," The Berkman Center for Internet & Society, Harvard University, February 1, 2016, https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.
[122] Aftab et al., "Information Theory," 5, 16-18.

Bibliography

"6.095/STS095: Selected items on Digital Telephony Act." Last modified October 19, 1997. http://groups.csail.mit.edu/mac/classes/6.805/articles/digital-telephony/digital-telephony.html.

Abelson, Harold. Anderson, Ross. Bellovin, Steven M. Benaloh, Josh. Blaze, Matt. Diffie, Whitfield. Gilmore, John. Green, Matthew. Landau, Susan. Neumann, Peter G. Rivest, Ronald L. Schiller, Jeffrey I. Schneier, Bruce. Specter, Michael A. Weitzner, Daniel J. "Keys under doormats: mandating insecurity by requiring government access to all data and communications." *Journal of Cybersecurity* (2015): 1-11. http://academiccommons.columbia.edu/catalog/ac:127127.

Ablon, Lillian. "Growing dependence on technology raises risks of malfunction." *Crain's,* July 9, 2015. http://www.crainsnewyork.com/article/20150709/TECHNOLOGY/150709895/growing-dependence-on-technology-raises-risks-of-malfunction.

AFP. "Google to Boost Android Encryption, Joining Apple." *Security Week,* September 18, 2014. http://www.securityweek.com/google-boost-android-encryption-joining-apple.

Aftab, O., Cheung, P., Kim, A., Thakkar, S., Yeddanapudi, N. "Information Theory: Information Theory and the Digital Age." Final paper, *Project History,* Massachusetts Institute of Technology, 2001. http://web.mit.edu/6.933/www/Fall2001/Shannon2.pdf.

Alberts, David and Papp, Daniel., eds."The Information Age: An Anthology on Its Impact and Consequences." CCRP Publication Series, 1997. http://www.dodccrp.org/files/Alberts_Anthology_I.pdf.

Apple. "A Message to our Customers." February 16, 2016, http://www.apple.com/customer-letter/.

Apple. "Amicus Briefs in Support of Apple." http://www.apple.com/pr/library/2016/03/03Amicus-Briefs-in-Support-of-Apple.html.

Apple. "Answers to your questions about Apple and security." http://www.apple.com/customer-letter/answers/.

Apuzzo, Matt and Benner, Katie. "Apple Is Said to Be Trying to Make It Harder to Hack iPhones." *The New York Times,* February 24, 2016. http://www.nytimes.com/2016/02/25/technology/apple-is-said-to-be-working-on-an-iphone-even-it-cant-hack.html?smid=fb-nytimes&smtyp=cur&_r=1&mtrref=undefined.

"Ask CALEA, Communications Assistant for Law Enforcement Act." June 22, 2011. https://askcalea.fbi.gov.

Barboze, David and Mozur, Paul. "New Chinese Rules on Foreign Firms' Online Content." *The New York Times,* February 19, 2016. http://www.nytimes.com/2016/02/20/business/media/new-chinese-rules-on-foreign-firms-online-content.html?_r=0.

Barrett, Devlin. "FBI Plans to Keep Apple iPhone-Hacking Method Secret." *Wall Street Journal,* April 26, 2016. http://www.wsj.com/articles/fbi-plans-to-keep-apple-iphone-hacking-method-secret-sources-say-1461694735.

BBC. "WhatsApp Brazil: Judge lifts suspension of messaging service." May 3, 2016. http://www.bbc.com/news/world-latin-america-36199489.

Benner, Katie and Wingfield, Nick. "Apple is Rolling up Backers in iPhone Privacy Fight Against FBI." *The New York Times,* March 3, 2016. http://www.nytimes.com/2016/03/04/technology/apple-support-court-briefs-fbi.html?_r=0.

Blaze, Matt. "Protocol Failure in the Escrowed Encryption Standard." AT&T Bell Laboratories, August 20, 1994. http://www.crypto.com/papers/eesproto.pdf.

Borgman, Christine. *Scholarship in the Digital Age: Information, Infrastructure, and the Internet.* Massachusetts: MIT Press, 2007.

Brodkin, Jon. "Report: 'Deeply divided' White House won't support anti-encryption legislation." *Ars Technica*, April 7, 2016. http://arstechnica.com/tech-policy/2016/04/white-house-reportedly-wont-support-anti-encryption-legislation/.

Burgess, Matt. "Bill Gates backs FBI in Apple's iPhone encryption battle." *Wired,* February 23, 2016. http://www.wired.co.uk/news/archive/2016-02/23/bill-gates-support-fbi-apple.

Burr, Richard and Feinstein, Dianne. Compliance with Court Orders Act of 2016. Discussion Draft. Released April 13, 2016. https://www.eff.org/document/burr-feinstein-encryption-bill-discussion-draft.

Clover, Juli. "FBI Used Security Flaw Found by 'Professional Hackers' to Crack San Bernardino Shooter's iPhone." *MacRumors,* April 12, 2016. http://www.macrumors.com/2016/04/12/iphone-5c-flaw-fbi-professional-hackers/.

Comey, James. "Going dark." Speech, Brookings Institution, Washington, October 16,

2014. https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course.

Comey, James. "Perceptions of Privacy." Speech, Kenyon College, Ohio, April 1, 2016, http://www.kenyon.edu/middle-path/story/perceptions-of-privacy/

Conger, Kate. "Burr-Feinstein encryption bill is officially here in all its scary glory." *Tech Crunch,* April 13, 2016. http://techcrunch.com/2016/04/13/burr-feinstein-encryption-bill-is-officially-here-in-all-its-scary-glory/.

Crocker, Andrew. "Worried about Apple? California Has a Bill That Would Disable Encryption on All Phones." Electronic Frontier Foundation, March 9, 2016. https://www.eff.org/deeplinks/2016/03/worried-about-apple-california-has-bill-would-disable-encryption-all-phones

Cushing, Tim. "Comparing Cell Phones To Houses Not Exactly Deterring Use of Generalized Warrants, Court Finds." *Tech Dirt*, January 20, 2016. https://www.techdirt.com/articles/20160116/14332433358/comparing-cell-phones-to-houses-not-exactly-deterring-use-generalized-warrants-court-finds.shtml.

Davidson, Amy. "Four Ways the Riley Ruling Matters for the N.S.A." *The New Yorker,* June 29, 2014. http://www.newyorker.com/news/amy-davidson/four-ways-the-riley-ruling-matters-for-the-n-s-a.

Debates of the Century. "National Security." YouTube video. Filmed April 26, 2016. Posted May 1, 2016. https://www.youtube.com/watch?v=-yoyX6sNEqs.

Dewar, James A. "The Information Age and the Printing Press, Looking Backward to See Ahead." The Rand Corporation, 1998. http://www.rand.org/pubs/papers/P8014/index2.html.

Draper, Nora., Hennessy, Michael., Turow, Joseph. "The Tradeoff Fallacy: How Marketers Are Misrepresenting American Consumers and Opening Them Up to Exploitation." New Annenberg School of Communication, University of Pennsylvania, June 2015. https://www.asc.upenn.edu/news-events/publications/tradeoff-fallacy-how-marketers-are-misrepresenting-american-consumers-and.

Edwards, Julia. "FBI paid more than $1.3 million to break into San Bernardino iPhone." *Reuters,* April 22, 2016. http://www.reuters.com/article/us-apple-encryption-fbi-idUSKCN0XI2IB.

"Encryption and Globalization." *The Columbia Science & Technology Law Review* XIII (2012): 416-481. https://iapp.org/media/pdf/knowledge_center/Encryption_and_Globalization.pdf.

Farivar, Cyrus. "Apple expands data encryption under iOS 8, making handover to cops moot." *Ars Technica,* September 18, 2014. http://arstechnica.com/apple/2014/09/apple-expands-data-encryption-under-ios-8-making-handover-to-cops-moot/.

Farivar, Cyrus. "Judge: Apple must help FBI unlock San Bernardino shooter's iPhone." *Ars Technica,* February 17, 2016. http://arstechnica.com/tech-policy/2016/02/judge-apple-must-help-fbi-unlock-san-bernardino-shooters-iphone/

Finklea, Kristin. "Smartphone Data Encryption: A Renewed Boundary for Law Enforcement?" CRS Insights, October 17, 2014. https://www.fas.org/sgp/crs/misc/IN10166.pdf.

Floridi, Luciano. "Google ethics adviser: The law needs bold ideas to address the digital age." *The Guardian,* June 4, 2014. https://www.theguardian.com/technology/2014/jun/04/google-ethics-law-right-to-be-forgotten-luciano-floridi.

Floridi, Luciano. *The Fourth Revolution: How the infosphere is reshaping human reality*. Oxford: Oxford University Press, 2014.

FTI Consulting. "Allstate/National Journal Heartland Monitor XXIV Key Findings." September 18, 2015. http://heartlandmonitor.com/wp-content/uploads/2015/09/FTI-Allstate-NJ-Heartland-Poll-XXIV-Findings-Memo-Sept-24-2015.pdf

Gasser, Urs., Gertner, Nancy., Goldsmith, Jack., Landau, Susan., Nye, Joseph., O'Brien, David R., Olsen, Matthew G., Renan, Daphna., Sanchez, Julian., Schneier, Bruce., Schwartztol, Larry., Zittrain, Jonathan. "Don't Panic, Making Progress on the 'Going Dark' Debate." The Berkman Center for Internet & Society, Harvard University, February 1, 2016. https://cyber.law.harvard.edu/pubrelease/dont-panic/Dont_Panic_Making_Progress_on_Going_Dark_Debate.pdf.

Gidari, Albert. "DOJ Misleads Court on the CALEA in the Apple Case." The Center for Internet and Society, Stanford Law School, March 11, 2016. http://cyberlaw.stanford.edu/blog/2016/03/doj-misleads-court-calea-apple-case.

Gleick, James. *The Information, A History, A Theory, A Flood.* New York: Knopf Doubleday Publishing Group, 2011.

Gleick, James. "The Information: A History, a Theory, a Flood | Talks at Google." YouTube video. Filmed March 17, 2011. Uploaded March 24, 2011. https://www.youtube.com/watch?v=iyOzSzcDwg8.

Hagemann, Ryan and Chang Andrew. "Encryption showdown: Burr-Feinstein vs. McCaul-Warner." *The Hill,* April 25, 2016. http://thehill.com/blogs/congress-blog/technology/277467-encryption-showdown-burr-feinstein-vs-mccaul-warner.

Hew, Alex., Kumor, Damian., Mislan, Rick. "Apple Has Already won. Now It Should Crack the San Bernardino iPhone." *IEEE Spectrum,* February 22, 2016. http://spectrum.ieee.org/view-from-the-valley/consumer-electronics/portable-devices/apple-has-already-won-now-it-should-crack-the-san-bernadino-iphone.

Huffington Post. "Google Antitrust." http://www.huffingtonpost.com/news/google-antitrust/.

Internet Association. "Internet Association, CCIA, and i2Coalition Filed Amicus in Apple Case." Press release, March 3, 2016. https://internetassociation.org/030316encryption/.

Internet Live Stats. "Internet Users." http://www.internetlivestats.com/internet-users/.

Kizza, Joseph. *Ethical and Social Issues in the Information Age*. London: Springer-Verlag, 2010.

Kranzberg, Melvin. "Technology and History: 'Kranzberg's Laws.'" *Technology and Culture* 27 (1986): 544-560.

Lee, Dave. "Facebook: Political bias claim 'untrue.'" *BBC,* May 10, 2016. http://www.bbc.com/news/technology-36254201.

Lever, Rob. "In Apple vs. FBI case, compromise appears elusive." *Phys Org,* March 6, 2016. http://phys.org/news/2016-03-apple-fbi-case-compromise-elusive.html.

Levy, Steven. "Battle of the Clipper Chip. *The New York Times,* June 12, 1994. http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html?pagewanted=all.

Limer, Eric. "Most Useful Podcast Ever: Why is the FBI Using a 227-Year-Old Law Against Apple?" *Popular Mechanics,* February 24, 2016. http://www.popularmechanics.com/technology/a19483/what-is-the-all-writs-act-of-1789-the-225-year-old-law-the-fbi-is-using-on-apple/.

Manhattan District Attorney's Office. "On Smartphone Encryption and Public Safety," November 2015. http://manhattanda.org/sites/default/files/11.18.15%20Report%20on%20Smartphone%20Encryption%20and%20Public%20Safety.pdf.

Markoff, John., Benner, Katie., Chen, Brian. "Apple Encryption Engineers, if Ordered to

Unlock iPhone, Might Resist." *The New York Times,* March 17, 2016. http://www.nytimes.com/2016/03/18/technology/apple-encryption-engineers-if-ordered-to-unlock-iphone-might-resist.html?_r=1.

McCaul-Warner Commission on Digital Security. https://homeland.house.gov/wp%20-content/uploads/2016/02/McCaul-Warner-Commission-One-pager-1.pdf

McConnell, Mike., Chertoff, Michael., William Lynn. "Why the fear over ubiquitous data encryption is overblown." *Washington Post,* July 28, 2015. https://www.washingtonpost.com/opinions/the-need-for-ubiquitous-data-encryption/2015/07/28/3d145952-324e-11e5-8353-1215475949f4_story.html .

McGarry, Caitlin. "Obama on encryption: 'It's fetishizing our phones above every other value.'" *Macworld,* March 11, 2016. http://www.macworld.com/article/3043553/security/obama-on-encryption-its-fetishizing-our-phones-above-every-other-value.html.

Murdoch, Steven. "Apple vs. FBI." University College London, April 20, 2016. https://www.ucl.ac.uk/news/headlines/0416/200416-apple-fbi.

New Media Institute. "History of the Internet." Last modified 2014. http://www.newmedia.org/history-of-the-internet.html.

Nunberg, Geoffrey. "James Gleick's History of Information." *The New York Times,* March 18, 2011. *http*://www.nytimes.com/2011/03/20/books/review/book-review-the-information-by-james-gleick.html?pagewanted=all.

Pfefferkorn, Riana. "The Burr-Feinstein Crypto Bill Would Gut Our Cybersecurity." The Center for Internet and Society, Stanford Law School, April 26, 2016. http://cyberlaw.stanford.edu/publications/burr-feinstein-crypto-bill-would-gut-our-cybersecurity.

Rago, Joe. "The White House should have avoided this legal and security showdown." *The Wall Street Journal,* February 19, 2016. http://www.wsj.com/articles/the-fbi-vs-apple-1455840721.

Rajamaki, Jyri., Knuuttila, Juha., Ruoslahti, Harri., Patama, Pasi., Viitanen, Jouni. "Building Trust between Citizens and Their Governments, A Concept for Transparent Surveillance of Suspects." European Intelligence and Security Informatics Conference (EISIC), 2015. http://www.europarl.europa.eu/stoa/webdav/site/cms/shared/2_events/workshops/2015/20151208/Transparent%20surveillance%20of%20suspects%20for%20building%20trust%20between%20citizens%20and%20their%20governments.pdf

Roberts, Siobhan. "Claude Shannon, the Father the Information Age, Turns 1100100."

The New Yorker, April 30, 2016. http://www.newyorker.com/tech/elements/claude-shannon-the-father-of-the-information-age-turns-1100100.

Savransky, Rebecca. "Snowden: Without encryption, everything stops." *The Hill,* May 1, 2016. http://thehill.com/blogs/blog-briefing-room/news/278320-snowden-without-encryption-everything-stops.

Schneier, Bruce. "Cyberweapons Have No Allegiance." February 25, 2015, https://www.schneier.com/essays/archives/2015/02/cyberweapons_have_no.html.

Shannon, Claude. "A Mathematical Theory of Communication." *The Bell System Technical Journal* 27 (July, October 1948): 379-423, 623-656. https://archive.org/details/bstj27-3-379.

Shannon, Claude. "The Bandwagon." *IRE Transactions – Information Theory* (1956): 3. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=1056774.

Shannon, Claude and Weaver, Warren. *The Mathematical Theory of Communication*. Chicago: University of Illinois Press, 1949.

Shu, Catherine. "Facebook 's Save Free Basics in India" Campaign Provokes Controversy." *Tech Crunch,* December 17, 2015. http://techcrunch.com/2015/12/17/save-free-basics/.

Smith, Aaron. "U.S. Smartphone Use in 2015." Pew Research Center, April 1, 2015. http://www.pewinternet.org/2015/04/01/us-smartphone-use-in-2015/.

Solana-Ortega, Alberto. "The information revolution is yet to come (an homage to Claude E. Shannon)." *AIP Conference Proceedings* 617 (May 14, 2002): 458-472.

Statista. "Number of smartphone users worldwide from 2014 to 2019 (in millions)." 2016. http://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/.

Supreme Court of the United States. Syllabus, Riley v. California. October 17, 2013. http://www.supremecourt.gov/opinions/13pdf/13-132_8l9c.pdf.

Swire, Peter and Ahmad, Kenesa. "Encryption and Globalization." *The Columbia Science & Technology Law Review* XIII (2012): 416-481.

The Constitution of the United States, The Fourth Amendment.

Townsend, Kevin. "California Quietly Drops Bill Requiring Phone Decryption." *Security Week*, April 15, 2016. http://www.securityweek.com/california-quietly-drops-bill-requiring-phone-decryption.

United States District Court for the Central District of California. "Government's Motion to Compel Apple Inc. to Comply with this Court's February 16, 2016 Order Compelling Assistance in Search." *Wired,* February 19, 2016, http://www.wired.com/wp-content/uploads/2016/02/Apple-iPhone-access-MOTION-TO-COMPEL.pdf.

Vaas, Lisa. "Google quietly drops promised encryption by default for Android Lollipop." *Naked Security*, March 4, 2015. https://nakedsecurity.sophos.com/2015/03/04/google-quietly-drops-promised-encryption-by-default-for-android-lollipop/.

Winston, Brian. *Media Technology and Society, A History: From the Telegraph to the Internet.* London: Routledge, 1998.

Yadron, Danny. "FBI confirms it won't tell Apple how it hacked San Bernardino shooter's iPhone." *The Guardian,* April 28, 2016. https://www.theguardian.com/technology/2016/apr/27/fbi-apple-iphone-secret-hack-san-bernardino.

"Years of the iPhone: An Interactive Timeline." *Time,* June 27, 2014, http://time.com/2934526/apple-iphone-timeline/.

Yeung, Raymond. *A First Course in Information Theory.* New York: Springer, 2002.

Figures & Tables