May 18th, 9:00 AM - May 21st, 5:00 PM

Commentary on “America vs. Apple: the Argumentative Function of Metonyms”: Defeasible Rhetoric: Networks, Security, & Metonyms

G Thomas Goodnight
University of Southern California

Defeasible Rhetoric: Networks, Security, & Metonyms: Commentary on "America vs. Apple: the Argumentative Function of Metonyms"

G. THOMAS GOODNIGHT
Annenberg School of Communication
University of Southern California
gtg@usc.edu

Abstract: The government took Apple to court to demand decryption of a terrorist cell phone. The warrant issued rested on the assumption that law enforcement should be able to do its work through extension of "access" across the population of encrypted *iphones*. Each phone exists as a defeasible (Rescher 1977) site whose cooperation (access) is assumed to be opened by the the manufacturer if directed to do so by government, unless cause can be shown otherwise. Defeasible argument couples rhetorically with metonymic force as a powerful argument trajectory. The reversal of burden of proof, now placed on the company to defend its encryption, permits the government to extend the scope of its power by turning cell phone companies into its helpers. This is the manner in which a government would "commandeer innocent third parties into becoming its undercover agents, its spies, or its hackers" (Goldman & Segall 2016). The test case was crucial for Apple, but it was resolved by the discovery of a third-party who could gather the information without the manufacturers complicity.

1. The dark problem

The twenty-first century communications revolutions generates expanding experiments, particularly at the next where the law has to grow to catch up with social activities. The law is a conservative institution that lags behind yet remains vulnerable too changes in the public practices. Airlines, railroads, telegraph services coupled with mining, forestry, agriculture and fishing to produce modern prosperity. Modern revolution also generated new challenges to adapt international, national, and local legal institutions to the web of complications attended to legal intervention when things go criminally or contractually amiss. So, too, with the cybersphere expands challenge to the police powers of the state.

> Unfortunately, those who commit crimes have not missed the information revolution. Criminals use mobile phones, laptop computers, and network servers in the course of committing their crimes. In some cases, computers provide the means of committing crime. For example, the Internet can be used to deliver a death threat via email; to launch hacker attacks against a vulnerable computer network, to disseminate computer viruses, or to transmit images of child pornography. In other cases, computers merely serve as convenient storage devices for evidence of crime. For example, a drug dealer might keep a list of who owes him money in a file stored in his desktop computer at home, or a money laundering operation might retain false financial records in a file on a network server. Indeed, virtually every class of crime can involve some form of digital evidence. (Hagan & Judish 1979)

Communication networks organization argument activities that depend upon an ostensible open system of exchange but that is actually drawn around of a series of borders through which property becomes defined and useful security is achieved. The interests of the legal system is in the capacity of network logs, email, word processing files and image files to "provide the

Bondy, P., & Benacquista, L. (Eds.). *Argumentation, Objectivity, and Bias: Proceedings of the 11th International Conference of the Ontario Society for the Study of Argumentation (OSSA), 18-21 May 2016*. Windsor, ON: OSSA, pp. 1-6.

government with important (sometimes essential) evidence in a criminal case" (Hagan & Judish 1979).

Shadow networks accompany all forms of human empire. Neo-liberal America is no exception. James Scott (1985, 1990) identifies "weapons of the weak" as a practice that depends upon challenging public transcripts with anonymous, ambiguous, seemingly passive but aggressive acts of disruption, vandalism and disturbance. The highway man was a romantic figure, escaping the constraints of industrialism and domestic life. So, too, the mysteries of criminal concealment and shadow populations renew themselves in an Internet world. The dark web is a term used to refer that are hidden deepen among web connections. These are constituted by friend-to-friend networks and popular services such as Freenet, I2P, and To (Dark Web…n.d.) The Silk Road offered an infamous case where subterfuge was underway with illegal drug dispersal. In the police discipline, the Internet is imagined as a space to conspire, hide secrets, and assemble plots. Jamie Bar (2014) described the dark net as an undergrounded constituted by subcultures that included "social media racists, cam girls, self-harm communities, drug markets, cryptoanarchists and transhumanists."

2. Surveillance society

Into the mix of suspicion about activities of criminals and hiddenness of evidence comes entered the institutional momentum of surveillance and communications control of the Patriot Act. The public was unaware of precisely how much Congress had capitulated to fears of terrorism. Media companies were reluctant to let their customers know about private media surveillance and data sales of behavior. The same media companies were even more reserved about giving up their complicity with government orders for data. James Clapper the head of the National Intelligence for the National Security Agency (NSA) that had just finished a massive phone sweep operation on U.S. Cellular and Verizon was asked by Sen. Ron Wyden directly at a March 12, 2013 hearing: "Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?" Clapper's answer: "No Sir." (Kessler 2013). Of course, the Senate had been informed of data capture programs had been going on since 2007. The protections were rationalized by claims that courts are involved in special cases, even though FISA courts are secret and turned down not so much as a single request; further, the information is described as metadata which makes it sounds harmless in the particular case—which of course it may be, until back traced to the source from which it's taken. Shortly to follow were the Snowdown leaks. It was revealed that the NSA was "harvesting millions of email and instant messaging contact lists, searching email content, tracking and mapping the location of cell phones. Snowden's leaks were not the last (England 2014). Credit card hacking soon followed as popular sport. The Panama papers were thrilling enough for a hundred journalists to keep secret and the story ripen for a year.

3. Fictions of presence & legitimation controversy

The communications industry in the United States plays a tricky game.

> Ever since Edward Snowden released a mountain of information about the extent of U.S. government secret surveillance, the battle has been growing between tech companies and the government over access to data… Apple, Google, Microsoft

> and others to lock down, or encrypt, data on smartphones and digital devices. (Woodruff 2015)

Encryption protects clientele. Perception of security are core to maintain the legitimacy of digital activities. The whole simulated apparatus works to the extent that users make a defeasible judgment. The absence of social presence is discounted by the assumption that intrusions by surveillance apparatus of business, government and others doesn't really make a difference. A more sophisticated judgment locates the lack of presence as possibly mattering, but its problems are subject to correction, once lack of actual presence of an other matters. In this context, efforts to guard privacy through encryption devices are key to maintaining the legitimacy of the whole normalized operation. Those comfortable with a digital augmentation of their lifeworld in the first place can remain comfortable, ever more dependent, upon the apparatus without worry—because there is no technological means of intrusion. The technical assurance of privacy is key to the legitimacy of the communications industry.

The interests of the state and industry are stressed to the breaking point when it comes to cybersecurity. The efforts of the state to put on access and control devices goes as far back as Clipper Ship technologies. Even with repeated efforts to whip of fears of Chinese and Russian sponsored hack operations, business has been reluctant to subject its projects to machine control. The government is granted access to stored data in sets of not well-publicized rules.

4. Defeasible phones & the politics of encryption

Into the mix of appearance and illusion, things noticeable and not, plopped the cell phone of a San Bernardino terrorist. There are events that explode over the front page, bringing together a clash of people, agencies, and publics at a particular location. The volatility of the cases, themselves, render the discourse of interest to expert and lay publics alike. Network argumentation becomes exposed when a case erupts that forces to strive to capture and work toward personal, institutional, and public ends. The case concerned the partially destroyed iPhone used by Syed Farook and his wife Tashfeen Malik who murdered 14 at a holiday luncheon. The government inserted then withdrew litigation against Apple. The arguments asserted the need to have the phone opened in order to achieve access to potential evidence. Apple had built the encryption coding device, so it was assumed that it could and should reverse engineer the code in order to get into the phone, without efforts that would destroy the information secured within.

Solving a "dark problem" was desirable for evidence-hungry investigators; however the politics of control are quite another for the public. In a networked world, however, an individual phone traffics metonymically in the orbits personal and national security concerns. PBS discussed the politics of encryption.

> **DAVID SANGER:** And that's why, to borrow your iPhone here, *this is a national security problem in your pocket, and in everybody's pocket*. So, for *99.9 percent of communications, the government wants you to encrypt more, because they don't want criminals to be able to get into your bank account*. Your whole life is on this phone, right?
> **WILLIAM BRANGHAM:** Right.

> **DAVID SANGER:** Everything, medical data, financial data, conversations back and forth with family members.
> And they're protected by that four-digit code you type in, which in turn creates a much longer encryption key. So, the question is, who gets to hold on to that key? And *Apple said, we don't want it. We want you to have your own key*. Well, the problem…
> **WILLIAM BRANGHAM:** We being the individual user.
> **DAVID SANGER:** The individual.
> So, if the FBI wanted your data, or the NSA wanted to go in and get it because they thought you were communicating with a terrorist [the dark problem], what Apple is saying, don't bring that warrant to us. Go give it to William, and have him give you the key. Well, of course, the FBI's view is, drug dealers, terrorists, they're not likely to turn over a key. (PBS 2015)

The argument for government access turned on a technical rule, however, not public demand. The United States federal statute, The All Writs Act 28 U.S.C. ʒ 1651 furnished the basis of arguing that private actors should be compelled to serve investigative evidence of the state—even when no longer attached to a property. The original form of the law was the Judiciary Act of 1789. It was modernized in 1989. The Supreme Court authorized The **All Writs Act** 28 U.S.C. ʒ 1651 authorizes the United States federal courts to "issue all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law." The act in its original form was part of the Judiciary Act of 1789. The modern form of the act was first passed in 1911 "and the act has been amended several times since then, but it has not changed significantly in substance since 1789" (All Writs Act, n.d.). A writ was acceptable if it met 4 tests: there were no alternative remedies, that it was offered in an established jurisdiction, that it was necessary or fitting for the case at hand, and overall agreeable to the usages and principles of the law. In particular, "the U.S. Supreme Court ruled in United States v. New York Telephone Co. (1977) that the act provided authority for a U.S. District Court to order a telephone company to assist law enforcement officials in installing a device on a rotary phone in order to track the phone numbers dialed on that phone, which was reasonably believed to be used in furtherance of criminal activity" (All Writs Act, n.d.).

The logic of the federal case was hooked into defeasible reasoning; that is the company should provide access unless they can show cause as to why the apparatus does not meet the conditions of a legitimate writ. The position is something like a *decree nisi*, a condition set up for a ruling upon a condition that a rule applies unless a fact arises that would otherwise obstruct it. A rule nisi (unless) is a court order "that does not have any force unless a particular condition is met—"typically, the condition is that an adversely affected party fail to provide satisfactory evidence or argument that the decree should not take effect" (Decree nisi, n.d.). Apple did not concede the case because the concession would shift presumption and burden of proof to the manufacturers who were interested primarily in controlling their own access to their data. Cindy Cohn of the Electronic Frontier's Foundation supported Apple by posing the paradox. "A proposal to protect our security by weakening our security is going in the wrong direction," she claimed. "If the government were to suggest that no one put locks on their doors because if we were a terrorist it would be harder to get into our house, we would think that was a bad idea." "This is pretty much the digital equivalent of that," she maintained (Mello 2015).

5. Conclusion: liberty & control

Apple put up a fight because IF IT HAD BEEN conceded that the corporation had an obligation to undo its own security systems, then in cases where there is prosecutorial interest it would face a series of undoing security codes—passing along government and private surveillance opportunities part to part to part. Cell phones were aligned in metonymic array carrying the stamp of open, constant surveillance possibilities by private corporations directed by state agencies, first in the United States then likely around the globe. The naming process used in the court identified millions of phones as the need for "access" in order to fulfill the obligation of a "warrant" justified by setting up the defeasible condition. Metonymic reasoning was capped by reducing to absurdity the condition. The logic of government access to phones mandating that locks be compromised is similar to government access to homes mandating that locks be removed—all in the name of security that protects from rare or imagined (imminent as anticipated at some point) terrorist invasions. The government found third source to gain the information. The argument remains. The Internet renders material objects that set sights for communication and means to connect subject to metonymic chaining, whether authorized by the open and hidden measures of the state or smuggled into dark, vast hidden communities of practice.

There are several implications of the paper by Mauer and Mauer. The rhetorical force of defeasible argument needs to be understood, particularly as systems of control scrape away protections to liberty. Defeasible is only understood incompletely when transferred from a form of reasoning to an instrument of argumentation. Institutions that deploy defeasible reasoning to anticipate and discount arguments need to be held to close accountability by the populations they purport to serve. The burden of showing cause to defeat the rule figures rhetorically into constructions of identity and the performance of getting counted. Is metonymy the only, chief, or just one of many tropes that animates defeasible security argumentation apparatus? Second, the Internet is a vehicle for the announcement, coordination, and publicity of activities that seem to be open. The net is far from that, particularly as clouds digitize vast numbers of words, things, and information. Routine filters contribute to a naïve confidence in the range of non-private activities and negative performances that it hosts. The exploration of efforts to connect actors who prefer to remain hidden, remote, anonymous remind us that "natural language" analysis is by definition based upon highly artificial systems of visibility, search, and disclosure. Third, Enlightenment values such as freedom, privacy, liberty are conflicted with neo-liberal practices that front libertarian entrepreneurial rhetorics with systems of appropriation, control, and isolating filters. Critical argument inquiry of the practices of apparently innocent informal logic invite candid appraisal and analysis. We owe a debt of gratitude to Lauer and Lauer for bringing these things to our attention.

References

All Writs Act (n.d.). Wiki. Retrieved from: https://www.wikiwand.com/en/All_Writs_Act. May 6, 2016.

Bartlett, J. (2014). *The Dark Net*. UK: Bill Heinemann.

Decree Nisi (n.d.). Wiki. Retrieved from: https://www.wikiwand.com/en/Decree_nisi May 6, 2016.

"Deep Web," "Darknet," "Dark Web," and "Darknet Markets" from Wikipedia. Retrieved from: http://www.thevoicebeforethevoid.net/deep-web-darknet-dark-web-and-darknet-markets-from-wikipedia/ May 6, 2016.

England, C. (2014). Internet privacy and censorship. Foursys. Retrieved from: https://www.foursys.co.uk/Pages/Article/internet-privacy-and-censorship#.Vy1BeIQrKM8 May 6, 2016

Goldman, D. and Segall, L. (2016, March 2). ACLU: FBI wants to "commandeer" Apple. CNN Money. Retrieved from: http://money.cnn.com/2016/03/02/technology/apple-fbi-support/ May 6, 2016

Hagan, E. & Judish, N. (1979). Searching and seizing computers and obtaining electronic evidence in criminal investigations computer crime and intellectual property section criminal division OLE Litigation Series. Retrieved from: https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf May 6, 2016.

Kessler, G. (2013, June 12). Clapper's least "untruthful" statement to Senate. *Washington Post* Retrieved from: https://www.washingtonpost.com/blogs/fact-checker/post/james-clappers-least-untruthful-statement-to-the-senate/2013/06/11/e50677a8-d2d8-11e2-a73e-826d299ff459_blog.html May 6, 2016.

Mello, J. P. (2015). Apple's Cook goes to the barricades on encryption. TechNewsWorld. Retrieved from: http://www.technewsworld.com/story/82906.html May 6, 2016.

Rescher, N. (1977). *Dialectics.* New York: SUNNY.

Scott, J. (1990). *Domination and the Arts of Resistance: Hidden Transcripts*. South Haven: Yale University Press.

Scott, J. (1985). *Weapons of the Weak: Everyday Forms of Peasant Resistance*. South Haven: Yale University Press.

Woodruff, J. (2015). Why tech companies may be winning the encryption argument. PBS. Retrieved from: http://www.pbs.org/newshour/bb/tech-companies-may-winning-encryption-argument/ May 16, 2016.