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

America vs. Apple: the Argumentative Function of Metonyms

Ilon Lauer

Thomas Lauer
Oakland University

America vs. Apple: the Argumentative Function of Metonyms

ILON LAUER & TOM LAUER
Western Illinois University
Department of Communication
USA
MI-Lauer@wiu.edu

Oakland University
Rochester, MI 48309-4493
School of Business Administration
USA
lauer@oakland.edu

Abstract: Metonyms are inference generating tools capable of instantiating normative frameworks. Our study of public argumentation surrounding iPhone encryption addresses the argumentative function of the metonym. Metonyms accomplish general and specific argumentative purposes. Generally, metonyms help define and redefine the argumentative framework for a dispute. Within a controversy, metonyms operate as inference generators. We isolate and analyze several metonyms and elaborate their warrant-generating valences.

Keywords: Metonymy, unlimited development, encryption, institutional argument

1. Introduction – crypto-war redux

Throughout the San Bernardino iPhone controversy and in public hearings conducted in 2015 and 2016, law enforcement representatives from the Justice Department, the Federal Bureau of Investigation, and other agencies emphasized the similarity between investigating personal property during a judicially-warranted home search and the extraction of smart-phone data under the same conditions (pursuant to a search warrant). They contended a judicially-approved order to unlock an encrypted phone simply extends the scope of the warrant into a new but decidedly similar realm to where warrants have always operated. While appeals emphasizing consistent application of the warrant process appear reasonable, there is no legislative precedent guaranteeing law enforcement personnel permanent access to data in an unencrypted form. A peculiar tension emerged from this position; Law enforcement representatives emphasized their consistency with earlier legislation—specifically, the Communications Assistance for Law Enforcement Act (CALEA)—at the same time they argued that new legislation is necessary because recent advances in encryption capacity necessitate third party cooperation in obtaining digital information.

Law enforcement advocates represented access to encrypted phones as a time-honored and legally sanctioned investigative procedure. At the same time, their legal briefs cited an absence of legislative authorization to justify rulings securing iPhone data. This strategy provoked some public suspicion and criticism, but it afforded the Justice Department the luxury of choosing the optimal cases to advance their position in public and legal fora. The San Bernardino iPhone case functioned as one such case. Because the county owned the encrypted phone in the dispute, a right to privacy claim was unlikely. Moreover, Syed Farook, the deceased user of the iPhone, was unable to assert any tenuous claim to privacy that could potentially be advanced. Enjoying general support for its investigation, the Justice Department could lose the case while still gaining public acceptance for its position. In fact, we contend that the Justice Department's decision to withdraw from its case following Apple's appeal—despite winning a favorable judgment from the Federal

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. 1-13.

District court—demonstrates that its public strategy was at least as important as its efforts to obtain a ruling. Rather than risk a higher court resolution that could resolve conflicting Federal District Court decisions in San Bernardino and Brooklyn, the Justice Department's withdrawal preserved the option to initiate other high-profile cases and garner additional public support by advancing new and refined arguments tailored for public consumption. The Justice Department may have retreated from the San Bernardino battle, but the second crypto-war is just heating up (Meinrath & Vitka 2014).

Argumentation advanced by law-enforcement supporters during the Department of Justice's public and legal campaign to secure access to an encrypted iPhone in San Bernardino emphasized the integral importance of the "warrant" a metonym connecting judicial authorization with criminal investigation procedures. Law enforcement advocates drew a range of inferences from this metonym to frame encryption as a hindrance to the investigative process and to compel decryption of Syed Farook's county-issued iPhone. To clarify the argumentative deployment of this term, we elaborate the extensions through which metonyms generate inferences, instantiate normative frameworks, and reconfigure the argumentative ground to shift presumption in a controversy. Metonyms advance both broad and specific argumentative purposes; metonyms operate broadly to configure or reconfigure the argumentative framework of a dispute; within a controversy, metonyms and their extensions operate more narrowly as inference generators for defeasible arguments. Simply put, metonyms are potent argumentative tools for advancing institutional aims.

2. Institutional argument

To perpetuate legitimacy and authority, governing agencies often elude public argumentation at the same time they affirm their dedication to deliberative processes (Doxtader 1995). Doxtader (1995) has encouraged argument scholars to appreciate the ways "institutions create self-replicating forms of argument that deter deliberation." Such self-replicating forms conform to the norms of their argument field, but we suggest that they typically pursue arguments from Unlimited Development, a commonplace that identifies setbacks or obstruction as a rationale for perpetuating and even further extending the hindered policy or philosophy. Perelman and Olbrechts Tyteca (1969, p. 288) call attention to the ways this argument process emphasizes the obstacles to a goal to advance the goal itself.

In arguments from Unlimited Development, the perpetuation and expansion of an ideal functions as a warrant for pursuing an action or securing a perspective. When advanced by institutional agents, such warrants generate arguments perpetuating and expanding the institution's scope. Perelman and Olbrechts-Tyteca (1969, p. 290) elaborate the ways the warrant conceptually stretches the meaning of the underlying values of the institution, giving these values a verb-like force: "In argumentation using unlimited development, the hearers are often more interested in the value which such argumentation confers on certain terms which fall short of the ultimate term, but are really the center of the debate, than they are in the ultimate, always receding, term in a given direction." The transformative process of embedding the argumentative end into the warrant has powerful effects.

Arguments from Unlimited Development are difficult to rebut, in part, because they direct disputation toward the obstacle to the ideal more than the ideal itself. This shifted focus effectively turns the table by modifying the perception of the institution's position. As Perelman and Olbrechts-Tyteca (1969, p. 289) explain, such argumentation is "often employed to transform

arguments "against" into arguments "for," to show that what was up to that point regarded as an obstacle is in reality a means for reaching a superior station." Perelman and Olbrechts-Tyteca (1969, p. 288) best explain the way such positions reverse the evaluations of their positions, noting that this line of argumentation seeks to "defend behavior which the hearers would be tempted to blame, were it not assigned a place in the protraction of that which they approve and admire."

Because rhetorical figuration transforms the meaning of concepts, it is integral to the process of institutional argument. Clarke (2005) documented the ways that definitions authorize institutional legitimacy. Heidt (2013, p. 248) has demonstrated how operative metaphors animate government agencies to influence the scope of their mission and he advises argumentation scholars to study the language governing institutions use to define their missions and roles: "Critical inquiry into the rhetorical forms like metaphor that authorize, extend, or reassert public policy can usefully expose those forms as antidemocratic tools that sanitize public conceptions and convert well-intentioned public policy into something else entirely." We add that the metonym's role in this definitional process is potentially more significant than that of the metaphor and offer our case study to demonstrate this claim.

3. Metonymy in argument

The term metonymy refers to the figure of speech that obtains its persuasive force through naming. Unfortunately, the traditional study of metonymy as a stylistic device has inhibited broader inquiry into its argumentative functions. Even though dialectic treatises never included metonym amongst the commonplaces, rhetorical scholars have long recognized naming as a potential source of inferences. Aristotle's *Rhetoric* (2007, pp. 183-4, 2.23.29) presented naming as the final common topic but only addresses warrants drawn from traits of proper names. Cicero's *Topics* (1976) excluded proper names, but identified a term's etymology as a potential source of inferences. Agricola's late-renaissance treatise of dialectic offered a more sustained treatment of the naming topic, but did little more than collocate earlier discussions of proper names and etymology (Mack 1993, p. 147). More recently, Schiappa (2003) explored the function of naming in definitional argument and documented both the bureaucratizing and domesticating force of names, demonstrating how names influence a definition's connotation (making nuclear weapons "friendly" through domestication) and how names insulate discourse from outside scrutiny (removing other nuclear weapons from public discourse through "bureaucratization").

These premises configure the argumentative ground for a controversy by naturalizing and then normalizing concepts. Meyer (2008, pp. 141-8) has detailed how the metonym embeds premises associated with the general circumstances of a concept (who, what, where, when, or why). In this way, the metonym configures and reconfigures the fundamental ground of the argument and establishes what is germane and not germane to a controversy. Perelman and Olbrechts-Tyteca (1969, pp. 172-3) identify metonyms as terms of substitution that periphrastically arguments. Perelman and Olbrechts-Tyteca (1969, p. 88) elaborated this cognitive process and noted its incompatibility with more traditional logical operations:

> The passage from the normal to the normative, which is common among those who base ethics on experience, has rightly been considered an error in logic. Nevertheless, it should be recognized as one of the valid foundations of argumentations, inasmuch as this passage is implicitly admitted, whatever the domain under consideration…. It is found also in all those terms which cover both

> membership in a group and the usual behavior of the individuals in this group: thus, depending on circumstances, the words "American" and "socialist" may refer either to a behavioral norm or to a normal behavior. Put another way, the more the metonym is seemingly typical, the more it starts to typify the membership class. Metonyms which appear to be appropriate and unproblematic are particularly potent in public settings because they strengthen a certain perspective. The passage from the normal to the norm is a phenomenon of common occurrence and seems to be taken for granted.

Ultimately, the metonym insinuates standards for evaluating the respective merits of examples and cases in an argumentative setting. An accepted metonym assumes a normative role in a dispute when it becomes the prototypical member of a particular category. Elaborating the cognitive processes detailed in linguistic study, Gibbs (1999, p. 66) summarizes the metonym's typifying process: "The most representative members of any category are termed prototypical members and these often 'stand for' or represent the entire category." An accepted metonym can influence the relevance of concepts in a dispute. Put succinctly, metonyms that best *fit* make *sense*.

Turning to our study of the argumentation surrounding encryption of digital devices, we trace the ways the search warrant, the ultimate exception to privacy protection, is reconfigured to justify decryption demands. Reconfiguration energizes the warrant process with verb-like force and transforms arguments against surveillance into arguments for decryption. This shift in presumption against encryption can best be understood by analyzing the inferences drawn from two metonyms and elaborating the links between inference generation and traditional metonymic processes of substitution; association of cause with effect (warrant for search) and container for contained (iPhone for digital data).

4. The warrant is the warrant – naturalizing the metonym

Despite public declarations of support for digital encryption, permanent access to digital data has long been a law enforcement ideal.[1] Implying that legal authority to collect electronic information

[1] The San Bernardino case is only the most recent flashpoint in a longstanding controversy. Over the past twenty-five years, Federal law enforcement agencies have expanded their respective missions by securing greater access to electronic data and digital communications. The opening salvos of the first crypto-war began in the early 1990s with argumentation aimed to secure electronic surveillance as a law enforcement prerogative. In 1990, the FBI initiated "Operation Root Canal," a campaign to expand the agency's ability to monitor tele-communications which ultimately resulted in the implementation of CALEA. Intelligence agencies saw encryption as an obstacle to these efforts, concerns evident in a series of memos from Brent Scowcroft, National Security Advisor at the time. On January 17, 1991, a memo written to Dick Cheney, the Secretary of Defense, William Barr, the Attorney General, and Robert Gates, Director of Central Intelligence, urged a two-step strategy, first securing law enforcement access to telecommunication, followed by efforts to bypass data encryption: "Justice should go ahead now to seek a fix to the digital telephony problem, and all parties should follow through on the encryption problem in about a year. Success with digital telephony will lock in one major objective; we will have a beachhead we can exploit for the encryption fix; and encryption access options can be developed more thoroughly in the meantime" (Schnier & Banisar 1997, 160–3). A follow-on memo to President Bush outlining the same issues garnered executive approval to monitor digital telecommunications. After securing access to telecommunications transmissions, law enforcement agents turned their attention to decryption. On May 26, 1992, a memo from William Sessions, FBI Director to the Attorney General pertaining to Secretary of Commerce Barbara Franklin stated that her help was critical for "…buttressing the National Institute for Standards and Technology, whose efforts in support of our digital signature standard (the first phase of our strategy to address the encryption issue) must be re-energized" (Schnier and Banisar, 210). These wide-ranging

has already been granted by Congress, recent testimony given by FBI director James Comey and Sally Yates, Deputy Attorney General of the Department of Justice (2015) insists that access to iPhone data ensures a balance between security and privacy that has existed for the past twenty five years. Presenting their position as a maintenance of the status quo, Comey and Yates (2015, p. 5) request legislative authorization for law enforcement agencies to "…continue to obtain electronic information and evidence pursuant to the legal authority that Congress has provided to us to keep America safe." Despite similarities in goals and purpose, the rhetorical stance assumed by those advancing law enforcement interests has deviated from the one taken in the first crypto-war; over the past two years, law enforcement advocates have diligently avoided associating their position with a request for decryption "keys." Instead, they advocate the integrity of the warrant, a metonym representing a cause and effect relationship binding a justification (legal authority to investigate) with the result (searching personal property). As the warrant metonym naturalizes the law enforcement perspective during the iPhone dispute, the demands of the criminal investigation process are bound to encryption and decryption issues. This link is integral to the constitution of the metonym, which contains three elements (a) warrant/authorization, (b) cause/effect relationship and (c) search (Fig 1). Law enforcement advocates have deployed a systematic set of arguments based in emphases and extensions of the warrant metonym in combination with the iPhone metonym (a container signifying the digital information it contains fig. 2). At different times in the dispute the extensions and intensity of these different elements influence and even alter the type of arguments associated with the term. In argumentative settings, these plastic qualities energize the seemingly stable warrant metonym.

Fig. 1 Warrant metonym

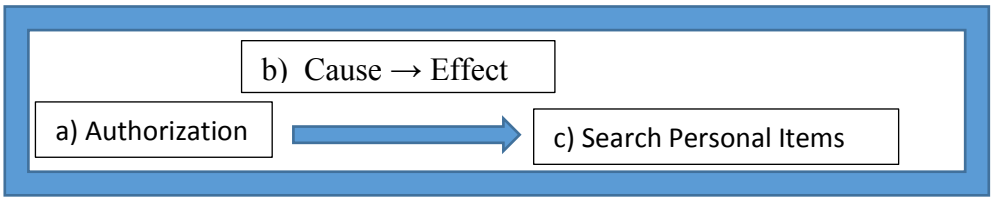
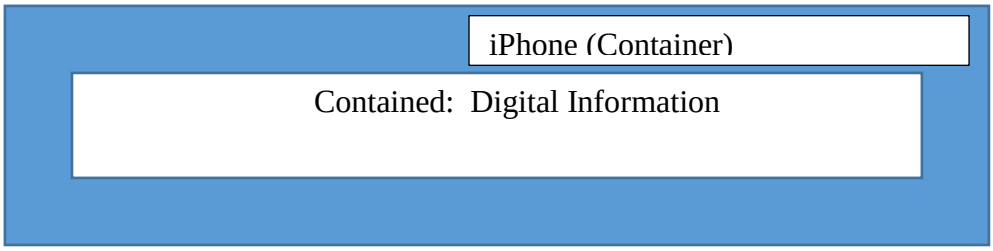


Fig. 2 iPhone Metonym



The warrant metonym resonates semantic values associated with legality, due diligence, and a rigorously objective procedure. These values make the law enforcement position more trustworthy. Testifying before the Senate Judiciary Committee a couple months after Comey and Yates, the New York County District Attorney, Cyrus Vance (2015, p. 11) identified Apple's encryption policy as a challenge to the public values associated with the search warrant process:

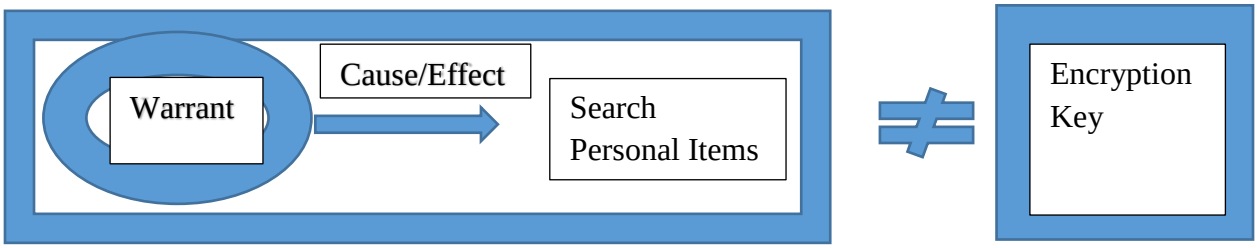
efforts to connect law enforcement activities to digital surveillance have consistently linked surveillance policy and goals to law-enforcement efforts.

> [T]he effect of Apple's encryption is that it prevents (i) the necessity of Apple responding to lawful government requests and (ii) the government from examining the contents of iDevices, even when an independent judge has authorized such disclosure by issuing a search warrant. Of course, a search warrant cannot be issued absent a showing of probable cause to believe that a crime has been committed and that evidence or proceeds of the crime might be found in the iDevice to be searched.

The initial shift in presumptions stems from these ethotic references. The fact that the warrant has already demonstrated probable cause suggests that opponents are probably wrong. Of course, this is excessively simplistic and naturally the arguments for or against the application of the warrant will have more influence than these immediate semantic resonances, but these resonances do color the exchange of arguments advanced by disputants on all sides.

One of the primary features of the warrant metonym is its emphasis upon the authorization of the search and its shifting of focus away from many of the results that follow from the metonym's application. In a public essay defending the FBI's position in the San Bernardino case, FBI Director James Comey (2016) categorically denied any desire to obtain decryption or access keys: "*We simply want the chance, with a search warrant,* to try to guess the terrorist's passcode without the phone essentially self-destructing and without it taking a decade to guess correctly. That's it. *We don't want to break anyone's encryption or set a master key loose* on the land." (para. 2, *emphasis added*) Emphasizing the "authorization" component of the warrant metonym and only vaguely alluding to the search process, such statements dissociate the warrant-based search from any mandate of key-escrow access (fig. 3). When the warrant metonym occupies the foreground it appears to be distinct from the authorization of keys, decryption, or any other type of mandated technical fixes. Indeed, when viewed simply as a legal justification, it becomes difficult to detect any of its metonymic properties.

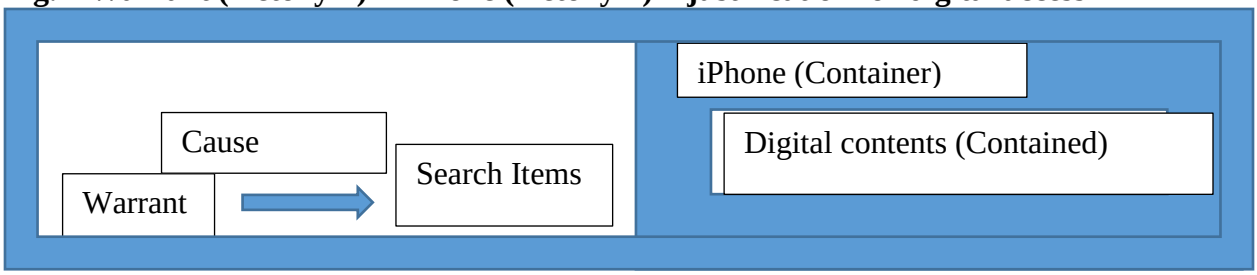
Fig. 3 Warrant dissociated from decryption



Even as the warrant metonym explicitly dissociates searching from the decryption process, its extensions produce inferences that entail access to information stored on digital devices. The designation of the iPhone metonym as the object of the search subjects both the container (iPhone) and contained (Digital information) to the purview of the warrant. (Fig. 4) Senator Dianne Feinstein and Congressman Pete Aguilar (2016) make this extension evident with a rhetorical question insisting that the iPhone falls within the scope of the warrant: "*Warrants executed in this investigation* have *exposed* every other aspect of the San Bernardino terrorists' lives; *why should they also not extend to the iPhone* simply because it's an Apple product?" (para. 12, emphasis added).

Justifications warranting a home search easily lend themselves to the demand for access to an encrypted phone: If a warranted search of a home is legally acceptable, a warranted search of any object found within the home should be equally acceptable. Identification of the metonym, iPhone, as the object of a search draws attention to the physical limits of the container and implies a finite limit to the material containing it (data). But the domain of digital information is practically infinite and the pairing of these two metonyms in this argumentative setting renders the containers into conduits. The device has become secondary to the data it contains. Seemingly confined to solitary objects, the metonym obscures the expansion of access to digital information *through* the digital device in addition to the information *in* it.

Fig. 4 Warrant (metonym) + iPhone (metonym) = justification for digital access



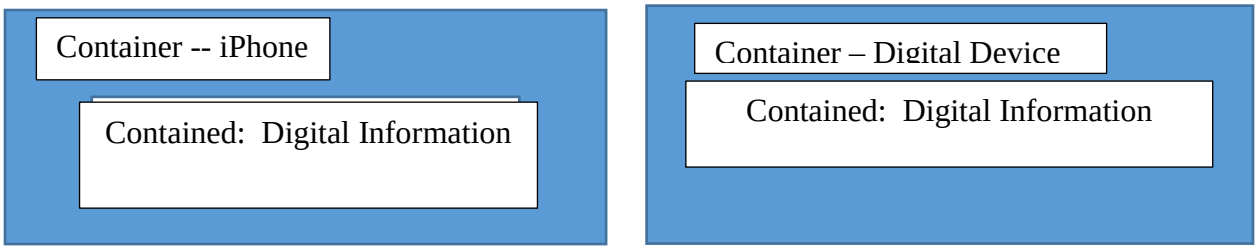
5. Configuring the norm: access to encrypted information

In defeasible arguments advancing the law enforcement perspective, the warrant metonym offers a normative basis for determining the unsuitability of encryption. New York District Attorney, Cyrus Vance, testified that law enforcement personnel simply seek the maintenance of conditions enabling criminal investigators to obtain digital information in an intelligible form. According to this view, encryption is not inherently problematic to law enforcement personnel; it only becomes so when it impedes the search. The San Bernardino court ruling followed this logic and called for Apple to provide technical assistance with encrypted data on Farook's iPhone. The U.S. District Court (2016) ruling explicitly ordered that: "Apple shall assist in enabling the search of a cellular telephone … (the "SUBJECT DEVICE") pursuant to *a warrant* of this Court by providing reasonable technical assistance to assist law enforcement agents in obtaining *access* to the data on the SUBJECT DEVICE" (para. 1-2, emphasis added). The San Bernardino court ruling advances the purpose of the original warrant and compels Apple to provide technical assistance with opening the phone.

Ensuring authorized searching of the iPhone contents depends upon access to encrypted information and justifies the demand that Apple modify its newest devices. For law enforcement officials, accessing the iPhone is a suitable beachhead for encroaching upon all digital information. The iPhone operates as a prototype; its fundamental similarity to all digital devices allows for equal treatment of all members of the class. The core logic that connects the search of the iPhone to the search of its contents creates the broader categorical basis for examining the contents of any digital device real or imaginary. Much of the alarm voiced by privacy advocates stemmed from the precedent-establishing nature of the San Bernardino ruling. Since the iPhone is a suitable prototype for every digital device, the same reasoning chain linking the warrant process to secure access of the encrypted contents of a digital phone extends to the encrypted contents of any digital device (Fig. 5). To elucidate this position, Nation (2016, para. 10-11) argued that the warrant process guaranteed access to the contents of all digital devices falling within this class:

> As noted, no digital data is truly secure, and we would all do well to realize that before we decide to store sensitive information on our *digital devices.* In fact, in our democracy, we the people have decided that *no information subject to a valid warrant is beyond reach.* We have, in the Constitution, provided for the protection of our privacy in the process required to obtain a valid warrant. We should not allow technical brute force *to frustrate* the government's legitimate efforts *to solve crimes*, especially crimes as reprehensible as terrorism." (emphasis added)

Fig. 5 Extension from iPhone to Digital Device



One of the primary objections to the San Bernardino ruling concerned its enlistment of Apple in advancing law enforcement efforts. Specifying the exact form Apple's technical assistance needed to assume, the District Court ruling rendered the metonym "warrant" an argumentative justification of third party decryption. The ACLU (2016, p. 1) Amicus brief voiced concerns with the government's use of "…third parties as its investigative agents to seek out information they do not possess or control…, law enforcement may not commandeer innocent third parties into becoming its undercover agents, its spies, or its hackers."

The court ruling did not simply require access to the iPhone; it entailed that Apple take active steps to ensure access by producing code enabling authorities to investigate the contents of the phone. Moreover, the prototypical nature of the phone enabled a categorical expansion to encompass all digital devices including applications on real and potential platforms. The warrant metonym was the basis for compelling Apple to design a way to access its product. In the San Bernardino ruling, the warrant went beyond a justification to investigate (cause) and instead became a demand for its success (effect). Despite risks to its public reputation, Apple devoted considerable public time and legal expense to resisting the San Bernardino court order because it feared that the compulsion to decrypt could extend to all Apple products, real and imagined. If the ruling stood, it could have set a precedent authorizing the decryption of all digital communication devices. As we observed earlier, Arguments of Unlimited Development redeploy the obstacle as a basis for perpetuating and advancing institutional goals. In the case of argumentation surrounding the San Bernardino case, the redeployment of encryption as an obstacle to the investigation enabled advocates to argue for expanding the scope of the search warrant process. Despite the potential to massively extend the scope of surveillance power, the role of surveillance in a democratic society was an omitted topic in the public discussion.

The language of the San Bernardino ruling, along with public argumentation supporting it, intensified the force of the search and animated it with the force to compel cooperation with the investigation. The reasoning advanced by the Justice Department lawyers and accepted by the District Court in the San Bernardino case associated verb-like properties with the warrant metonym. In effect, their arguments render one component of the warrant metonym "search" into

a gerundive form "searching." Unlike a search which has implicit temporal limits, the court ruling demands an absolute perpetuation of the investigative process, searching. Reversing the substitution process while still concealing the decryption aim, the metonym of the warrant binds an explicit cause (investigatory power) with an implicit effect (surveillance power), conflating *an authorization to access* with *quality of access*.

5. Reconfiguring encryption: decryption as duty

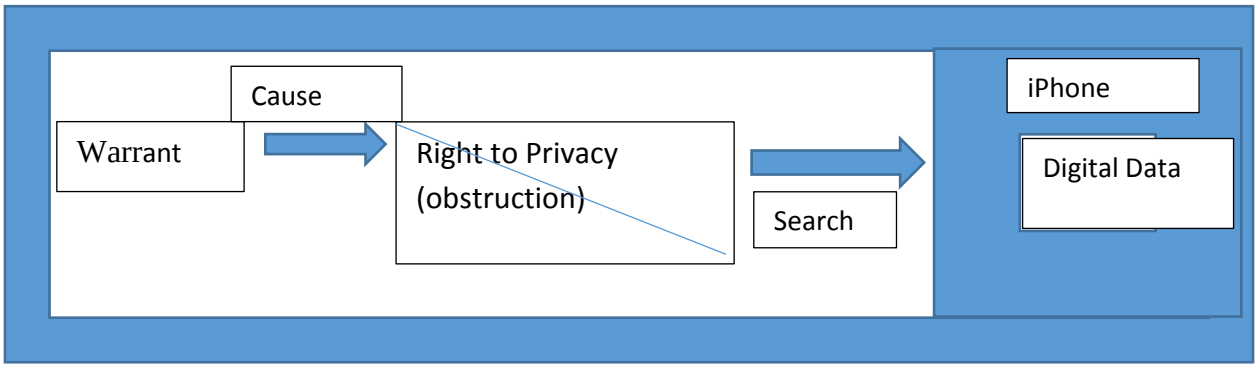
Arguments identifying the warrant process as a normative standard for evaluating encryption arguments effectively reverse presumption, rendering encryption the problem that necessitates third party cooperation with decryption efforts. In our final section, we isolate the way the warrant metonym reversed presumption by generating inferences supporting defeasible arguments that presented decryption as a moral, legal, and political obligation. Reconfiguring decryption as obligation proceeds in two stages. First, the warrant metonym strongly binds the cause (justification) with the effect (search) and bypasses legal impediments to this process (Fig. 6). Second, the double negative "cannot obstruct" is transformed into the affirmative "must assist" after imposing a law enforcement perspective on encryption questions (fig. 7). When the warrant metonym lays a normative foundation for evaluating encryption arguments, this framework produces an interesting double negative—this double negative is the product of framing encryption as an obstruction or impediment in combination with the warrant's impetus to search which negates any obstruction. We detail these two negations and elaboration the implications of their combination.

The initial negative "cannot hinder" emphasizes the government's position that the invocation of a right to privacy cannot impede the causal relationship between the warrant and the search. For instance, a *Daily News* (2016, para 21-22) editorial defending the constitutionality of the warrant process singles it out as an exception to privacy considerations:

> But *Americans have never had the right to absolute privacy* from government intrusion. *That's why courts can issue search warrants* in accord with the Constitution. It's also why the judge in the San Bernardino case used a federal statute to require Apple to fulfill Cook's stated commitment to comply "with valid subpoenas and search warrants. *(emphasis added*)

From the standpoint secured by the warrant metonym, this argument insinuates a negated privacy claim into the metonymic framework (fig. 6). In effect, the negation extends to any claim or justification that hinders the investigative process.

Fig. 6 The warrant process negates the right to privacy

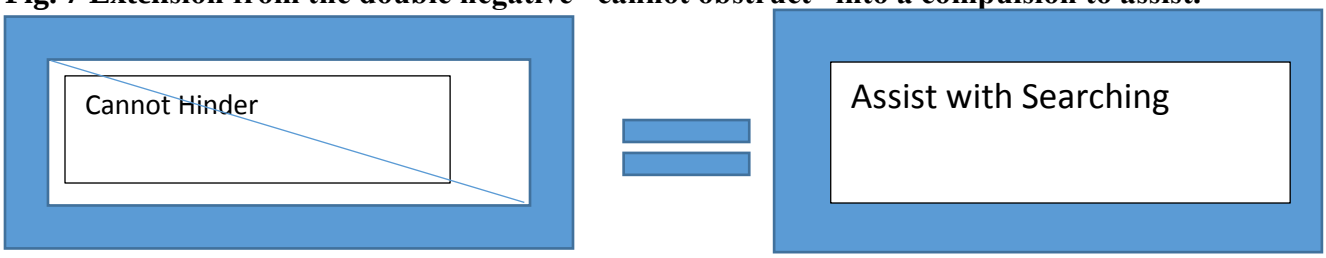


As the model illustrates, when the warrant metonym assimilates an objection into its framework it automatically reconfigures and negates it. Law enforcement representatives argued the Apple Corporation's installation of strong encryption in all of its operating systems shielded criminals and terrorists from criminal investigation. Vance (2015, p.11) asserted that the encryption capacity of newer iPhone versions nullifies the search warrant process: "Every home can be entered with a search warrant. I cannot think of another device that has been knowingly designed in a way to prevent *lawful* government inspection" (emphasis added). Vance's position can be rendered easily into a standardized form:

> Premise: The law allows for warranted searches of iPhones
> Premise: Encryption obstructs these warranted searches
> Claim: Encryption obstructs the law

Here the warrant process is exclusive with encryption. The warrant metonym refigures encryption design as obstruction. Instead of recognizing encryption as part of the product design that protects the customer, when refigured as an obstruction, encryption stands as a hindrance that necessarily must be overcome. Since warrants are legally authorized law enforcement tools, encryption effectively obstructs the investigatory process; by extension, securing access to digital information necessitates unimpeded and ultimately decrypted information. A shift in presumption follows the reconfiguration of the double-negative "cannot obstruct" into the affirmative "obligation to assist with searching." Here is where the presumption shifts away from encryption and towards the demand that companies facilitate decryption efforts. This reversal takes place because encryption and decryption cannot coexist. When encryption is configured as obstruction, the negation of encryption inevitably entails some form of decryption. Once the metonym of the warrant achieves normative standing, it exerts a teleological force on subsequent argumentation. In other words, the warrant metonym demands a search and in the domain of digital information this entails reversing any obstructions that inhibit perpetual searching capacity. (fig. 7)

Fig. 7 Extension from the double negative "cannot obstruct" into a compulsion to assist.



The warrant metonym was the conceptual anchor enabling advocates of the law enforcement position to advance defeasible arguments obliging Apple to comply with the San Bernardino ruling. These arguments advanced ethical, legal, and political justifications compelling Apple and, by implication, all third party designers of digital information to comply with the investigatory process when summoned. Nation (2016, para. 6-7) follows this line of reasoning, seamlessly moving from a negated right to privacy to the compulsion to help:

> Once a valid warrant has been issued, the right of privacy ends. Apple, like any other citizen, has an obligation to assist the government in any way that it can to

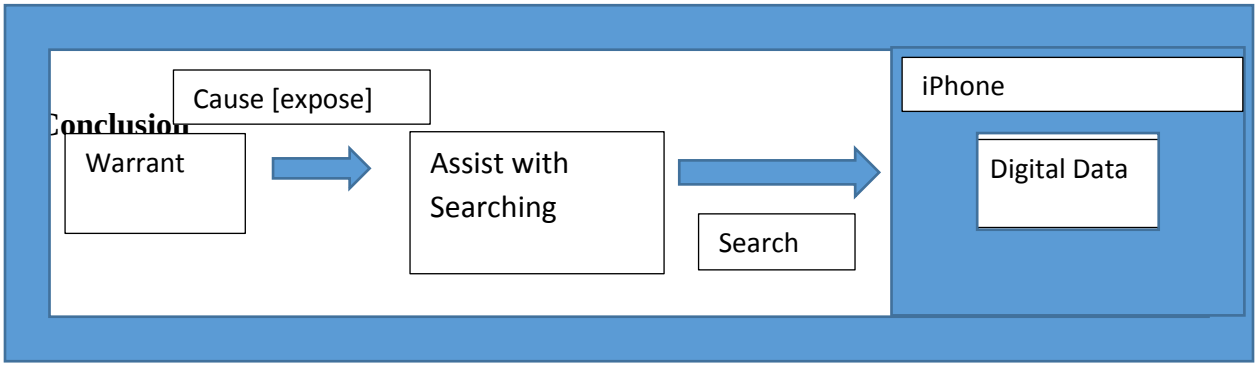
> implement the warrant. Moreover, the burden placed on Apple to write the software necessary to overcome its own encryption is a direct result of Apple's own conduct in designing the encryption in the first place.

Similarly, such negation of obstruction guides prosecutor Eric Zahnd's (2016, para. 10-11) editorial urging Federal legislation requiring third party assistance with the court warrant process:

> As the president urged, tech companies like Apple and Google must act now to open up their devices to lawful searches. Such *searches could only be carried out after a judge issues a search warrant* finding probable cause to believe that a device contains evidence of a crime. *And if the tech companies won't work cooperatively with law enforcement to make the searches possible, Congress must pass legislation to require it.* (emphasis added)

With minimal and barely noticeable inflection, the warrant metonym assimilates objections, presents them as obstacles to the goals of the metonym (searches) and reconfigures them to warrant assistance. (fig. 8)

Fig. 8 The "warrant" assumes the (ethical/legal) force to compel cooperation



Over the past two years, representatives from the law enforcement community have called for a new "conversation" regarding the role of encryption and they set the tone for this conversation by distancing themselves from earlier requests for encryption keys and by limiting their position to maintaining the integrity of the warrant. Because the fitness of the warrant as a metonym for the search process is determined by the extent to which it appears natural, the warrant has become a pivotal metonym in public contestation. A request to keep a key to someone else's property is less natural than an insistence that the property be accessible, but both embed the shared assumption that law enforcement officials have a right of access.

Arguments advancing the law enforcement perspective have pursued expanded surveillance power without expressing this ideal as an ultimate goal. Instead justifications for access reposition the telos of the search warrant and use it to justify securing access to encrypted phone data. Such repositioning has circumscribed the scope of the public debate; public argumentation largely concerns the technical and legal relationships between encryption and security. In other words, the warrant metonym has helped to confine the debate to whether companies should be compelled to develop the technological capacity to facilitate government monitoring of private communication. Public hearings, court arguments, editorials, and public

statements rarely consider the ultimate role of government surveillance despite the fact that permanent access to smart-phone data guarantees the continued relevance of traditional law enforcement agencies in the digital age. Despite considerable opposition to excessive surveillance, there has been little discussion of the role of continued surveillance and monitoring of electronic activities.

Use of metonyms in public argumentation renders certain perspectives normal and salient. Through repeated usage, seemingly natural terms become normal and ultimately normative, determining what operates as common sense in a given controversy. In argumentative settings, metonyms have elastic qualities that facilitate the advancement of an argumentative position and also determine the conditions of the controversy. Our study extends scholarly explorations of the connections between rhetorical figuration and argumentation by elaborating the way metonyms formulate and advance the argument of unlimited development and perpetuate institutional power.

References

ACLU, Amicus Curiae. (2016, March 22). Retrieved from https://www.eff.org/document/apple-fbi-all-writs-aclu-amicus

Apple's burden of proof: What Tim Cook's company must explain to the FBI and the public about iPhone encryption. *Daily News*. (2015, February 16). Retrieved from http://www.nydailynews.com/opinion/apple-burden-proof-article-1.2535427

Aristotle. *Aristotle's Rhetoric: A Theory of Civic Discourse*. (2007). (Trans.) G. A. Kennedy. Oxford: Oxford University Press.

Cicero. *Topica*. (1976). (Trans.) H. M. Hubbell. Cambridge: Harvard University Press.

Clarke, L. (2005). Contesting Definitional Authority in the Collective. *Quarterly Journal of Speech* 91, 1-36.

Doxstader, E. (1995). Learning public deliberation through the critique of institutional argument. *Argumentation and Advocacy* 31, online.

Feinstein, D. and Aguilar, P. (2016, March 3) Apple is threatening our national security. *Time*. Retrieved from http://time.com/4246499/apple-national-security/

Gibbs, R. W. Speaking and thinking with metonymy. In: K. Panther & G. Radden (Eds.), *Metonymy in Language and Thought* (pp. 1-76, Ch. 2), Amsterdam: John Benjamins.

Heidt, S. J. (2013). Presidential rhetoric, metaphor, and the emergence of the democracy promotion industry. *Southern Communication Journal* 78, 233-55.

Macagno, F. (2014). Manipulating emotions: value-based reasoning and emotive language. *Argumentation and Advocacy* 51, 103-22.

Macagno, F. and Walton, D. (2014). *Emotive Language in Argumentation*. Cambridge: Cambridge University Press.

Mack, P. (1993). *Renaissance Argument: Valla and Agricola in the Traditions of Rhetoric and Dialectic*. Leiden: E.J. Brill.

Meinrath, S. and Vitka, S. (2014). Crypto War II. *Critical Studies in Media Communication* 31, 125-8.

Meyer, M. (2008). *Principia Rhetorica: Une Théorie Générale de l'Argumentation*. Librarie Arthème Fayard.

Nation, G.A. (2016, February 27). Apple hissy fit about money, not principle. *Philadelphia Inquirer*. Retrieved from http://articles.philly.com/2016-02-27/news/70977702_1_encryption-hissy-privacy

Perelman, C. and Olbrechts-Tyteca, L. (1969). *The New Rhetoric: A Treatise on Argumentation*. John Wilkenson & Purcell Weaver (Trans.), Notre Dame: Notre Dame University Press.

Schiappa, E. (2003). *Defining Reality: Definitions and the Politics of Meaning*. Carbondale: Southern Illinois University Press.

Schneier, B. and Banisar, D. (1997). *The Electronic Privacy Papers: Documents on the Battle for Privacy in the Age of Surveillance*. New York: Wiley & Sons.

U.S. District Court of Central California Ruling, February 16, 2016, Downloaded from https://www.justsecurity.org/wp-content/uploads/2016/03/FBI-Apple-Magistrate-Order.pdf

Vance, C. R. (2015). Written testimony for going dark: encryption, technology, and the balance between public safety and privacy. July 8, 2015. Retrieved from https://www.judiciary.senate.gov/download/07-08-15-vance-testimony

Yates, S. Q. and Comey, J. B. (2015). *Prepared Remarks for Going Dark: Encryption, Technology, and the Balance Between Public Safety and Privacy*, Senate Judiciary Committee, July 8, 2015. Retrieved from https://www.judiciary.senate.gov/download/07-08-15-yates-and-comey-joint-testimony

Zhand, E. (2016, January 1). Cell phone encryption threatens us all. *Saint Louis Post-Dispatch*. Retrieved from http://www.stltoday.com/news/opinion/cell-phone-encryption-threatens-us-all/article_11a8c54e-24af-5a9d-b3b3-20ee2c3d9082.html