Beyond Sociomaterial: An Alternative Approach to Theorizing About Digital Artifacts

Full paper

Mark-David McLaughlin
Bentley University/Cisco Systems
mclaugh_mark@bentley.edu

Abstract

Information Systems researchers often study artifacts in light of their purpose, use, and effects. Their research is often conducted relying on a socio-technical or sociomaterial based ontology. For these realism-based approaches, ever-present security vulnerabilities, conflate the properties of the digital artifact making it impossible to conceive of a universal artifact. This paper explores how the types, tokens, and properties of IT artifacts change because of these vulnerabilities. This problematic condition for realism can be resolved by the adoption of agential functionalism. A functionalist views the type and token of an artifact by the function that it performs which results in a more consistent ontology when considering the impacts of security events. This move beyond materialism considers the properties of the IT artifact important but atheoretical allowing researchers to focus on the artifact's purpose, use, and effects. Ultimately, this ontology allows research to retain a type/token distinction necessary for generalized theories.

Keywords

Functionalism, IS security, ontology, philosophy, realism, sociomaterial, socio-technical

Introduction

Most IS researchers agree that IT artifacts should be studied in light of their purpose, use and effects. Thus far, philosophy-informed IS research has drawn on a range of theories, from Cartesian socio-technical to realism-based sociomaterial. The field has not yet reached a consensus regarding which philosophical approaches are best suited to investigate how and why digital artifacts influence user perceptions, IS adoption, ongoing use, and other important questions. This results in an incomplete ontology (the existence, features, and relations of entities) to guide IS research. This paper proposes that a functionalist view from the philosophy of the mind can serve as a useful approach to theorizing about the IT artifact.

One important IS question that has not yet been studied from a philosophical perspective is: How does the nature of an IT artifact change when a malicious actor exploits a security vulnerability? Herein, I propose that a functionalist approach provides a more consistent ontology for studying this question and other underexplored questions in IS research.

Employees, customers, citizens, and other users trust organizations to be guardians of their personal information, and in general, economic systems require reliable technology infrastructures. Yet, security breaches are an ever-present threat; the US Government Accountability Office reported that American businesses lose more than $400 billion a year from cyberattacks. Modern hackers are using increasingly sophisticated attack methods against business services and networks (Wong et al. 2012). Also, black markets have developed (Kannan and Telang 2005) which include auctions for tools designed to exploit vulnerabilities and conduct attacks. These tools and new markets increase the likelihood that malicious parties will successfully exploit system vulnerabilities (Ozment 2004). One study reported that users and managers perceive security threats to be high risk, and this perception in turn reduces their willingness to adopt IT solutions which lack robust security features (Zhu et al. 2006). Indeed, IS Security has become
such a monumental concern that United States President Obama proposed that the 2014 fiscal year budget for cyber security initiatives be increased by 21% (to $4.7 billion).

A recent review of IS security research reported that studies published in the IS Senior Scholar’s Basket of eight influential journals conceptualized security in a variety of ways, and papers within a particular research stream favored similar research methods (McLaughlin and Gogan 2014). Likewise, similar ontologies were used in studies within a particular research stream. Prior IS security research has explored the design, implementation and effectiveness of various information security policies and controls governing data protection, system access and availability (Lewis and Byrd 2003; Siponen and Iivari 2006); how organizations protect IT networks and data (Fernandez-Medina et al. 2007); and how security requirements impact vendor selection (Arora and Forman 2007). Each of these focus areas has a nuanced definition of security and the ontology of the IT artifact. Without a solid ontological foundation, attempts to generalize across studies are fundamentally flawed. Alarmingly, because of a lack of common epistemology in security studies, the necessary ontology of the artifacts changes if one is studying types (generalities) or tokens (particulars). Research that focuses on tokens and then formulates general theories needs to consider ontological changes that account for potential security issues impacting the IT artifact. In order to accomplish this, IS researchers should abandon the materiality notion of security as a “property of an IT artifact or system” and embrace security as a “function that an IT artifact performs”.

**Realism and the Sociomaterial**

The approach of many IS studies reflect Rene Descartes’ dualism or view that the universe consists of independent entities of mind and matter. For Descartes, the world consists of “in here” (adopted in IS research as *properties relevant to user intent*), and “out there” (*properties of an artifact without considerations of use*). Sociologist Bruno Latour (1987) rejected the Cartesian view; he argued that the IT artifact should not be viewed as “out there,” since technology features reflect only potential until they are put to use. However, IS studies consistent with Latour’s view subsequently drifted so far from the IT artifact that multiple calls were made to “return to theorizing about artifact” (Benbasat and Zmud 2003; Orlikowski and Iacono 2001). There was a general sense in IS research that culture, language, and discourse were all significant, but “matter did not matter anymore” (Barad 2003). Latour argued that the artificial distinction between epistemologies be removed in favor of a view that people, ideas, artifacts, and nature are linked together in an intricate network that develops and gains acceptance over time (Latour 1987). This change in ontology paved the way for some IS scholars to consider a view of the digital world that cannot be defined by that which is outside the mind—the digital world itself is merely a manifestation of intent—a reflection of human agency. This sociomaterial view of the IT artifact has been widely accepted by Galliers (2014), Leonardi (2007, 2013), Newell (2011), Orlikowski (2009; 2008), Scott (2013, 2014), Wagner (2010), and many others.

The Sociomaterial approach is firmly planted in one of two variations of realism, which in turn are based on two fundamental realistic aspects, *existence* and *independence*. Put simply, an object exists with all its properties, independent of an individual’s belief of its existence—language, culture, discourse, and conceptual schemas do not alter the essence of an object or its properties.

**Agential Realism**

Sociomaterialism relies on the concept of *agential realism* to take into account individual perceptions and uses of IT artifacts. Agential realism is based on Karen Barad’s work (1996). A key tenet of agential realism is the concept of “agency,” which is based on the relationship of an individual and an artifact. In this view, a technical artifact can be understood by how people use and interact with it. Like other sociomaterialists, Barad saw artifacts as shaping people and people shaping artifacts in interactions comprising the relationship. Barad further noted that researchers create artifacts to observe and measure the world around them, and that an individual’s perception of reality is *nothing more than renditions of reality* created by the instruments used to observe a phenomenon. Thus researchers’ views of reality are constructed inter-subjectively with the tools and processes used to describe phenomena. For example, astronomers created radio-telescopes to measure electromagnetic disturbances generated during celestial events. Since humans cannot detect these signals through their visual or audio senses, patterns in radio waves are converted to sounds or graphed as sine functions to provide a representation of changing amplitudes and frequencies. The radio astronomer’s ability to observe, understand, and describe the
signals is entirely dependent on these representations of the universe, as provided by the tools the astronomer used to capture and represent it.

It is important to recognize that for Barad, reality does not equal perception. Instead agencies of observation comprise an epistemological and ontological framework which emphasizes the inseparable nature of material and semiotic objects (Barad 1996). For Barad, researchers are “co-authors of the phenomena they are considering, agencies are seen to be products of the knowledge-making process as opposed to the properties of any specific actor.” Specifically, Barad describes these phenomena as:

“not merely mark[ing] the epistemological inseparability of ‘observer’ and ‘observed’; rather, phenomena are the ontological inseparability of agentially intra-acting ‘components.’... A specific intra-action (involving a specific material configuration of the ‘apparatus of observation’) enacts an agential cut (in contrast to the Cartesian cut—an inherent distinction ‘between subject and object) effecting a separation between “subject’ and ‘object.’...the agential cut enacts a local resolution within the phenomenon.” (Barad 2003)

Agential realism has been applied in IS research and contends that the digital world is not separate from its use—it is embedded and emergent; therefore, it is not entirely determinate (Ciborra 2002). The fundamental premise of this argument is that researchers cannot study IT artifacts without considering the interdependence between the artifact and human agent. In this view, the ontological Cartesian separation of individuals and technology used in early socio-technical research gives way to the notion of constitutive entanglements (Orlikowski 2007). Objects are simultaneously social and material—there are no inherent differences between the social and the material (Latour 2005). Orlikowski has further described this as “there is no social that is not also material, and no material that is not also social” (2007). Proponents of this view would not study the properties and affordances of a smartphone storing financial data (a digital safe), for example, without also considering how users interact with the device along with each of its properties and affordances. Likewise, we cannot understand how users protect data and software from security threats without also examining the properties and affordances of both the protected digital objects and of the IT artifacts that are used to provide the protection.

Even though Barad’s agential realism approach seems to be compatible with a view of the world that accounts for a separation of the social and the artifact through the notion of agential cuts, researchers have found it difficult to apply to their studies. Therefore, some scholars have been highly critical of it and supported critical realism as a solution to this dilemma.

**Critical Realism**

Mutch (2013) recently deemed agential realism “too laden with dense philosophical concepts,” and too difficult for researchers to operationalize philosophically inter-dependent entities. Many studies have resorted to the earlier socio-technical approach, in which the social and material are not mutually constituted, but instead defined by a Cartesian cut (Faulkner and Runde 2012; Leonardi 2012; Wagner et al. 2010). Mutch further argues that agential realism does not acknowledge how practices change over time and does not acknowledge those relationships that are not mutually constitutive. Mutch proposes that an alternative philosophical stance, critical realism, may be more appropriate for studies of digital artifacts. For a detailed response to Mutch’s criticism, see Scott and Orlikowski (2013).

Critical realism accepts the possibility of a reality that exists beyond human knowledge or conscious experience (Bhaskar 1979). In that sense, critical realism acknowledges that some of an artifact’s properties may not (yet) be perceptible with existing tools, and that these properties can be manipulated outside of individual perception. In other words, true to its roots in realism, critical realism contends that artifacts’ properties do exist independently of their observation. Critical realism also allows for the possibility of different perspectives on reality (as opposed to multiple realities) that are endlessly renegotiated with varying meanings and intentions (Putnam 1991). In this sense, critical realism is not entirely incompatible with agential realism. However, the two perspectives differ in how they treat human intent and properties of the artifact. Critical realism sees two separate entities that appear to become inseparable over time, whereas agential realism sees human agency and artifacts as being mutually constructed (Leonardi 2013).
Problems with Realism

Both agential realism and critical realism seem like plausible approaches to studying the properties of IT artifacts. However, the intrinsic properties of the type found in both forms of realism break down when taking into account the impact of security in the digital world. Security issues allow attackers to dynamically alter (almost boundlessly) the properties of digital artifacts. These modifications were not intended by the software’s creator or desired by the user and the changes are often outside the user’s perception. A physical safe and a smartphone acting as a digital safe are used to illustrate this counter-intuitive breakdown of realism by discussing the philosophical concepts of types, tokens and properties.

Types and Tokens

In order to illustrate the type token distinction, consider the simple pattern:

\[ X O X O X O X O X O \]

One view of this sequence is that it was constructed from two different letters \([X, O]\) each representing a type. Alternatively the sequence could be considered as ten individual letters representing five instances or occurrences of each type, referred to as tokens. While this is a simplistic example, in more complex artifacts, a type is conceptualized as the set of its tokens, containing all possible properties of the tokens (Quine and Quine 1987). This seems like a straightforward concept, but it is debated. A realist defines a token as the instantiation of an object and a type as the abstract object that is not located anywhere in space or time. This is consistent with the approach of Bromberger (1988), Halle and Mohanan (1985), Katz and Postal (1991), and Wetzel (2006). A nominalist view, in line with Goodman and Quine (1947) or Carnap (1991) would argue that there are no general tokens, only classes (non-spatiotemporal sets of tokens). Similarly, Armstrong (1988), Lewis (1972) and Forrest (1987) have debated the presence of a structural universal, or a type of which there are no tokens, but these considerations and debates are beyond the scope of this paper.

Security and Artifact Properties

A definition of security as it relates to an artifact is needed before we can examine why the exploitation of security vulnerabilities demands that we change the ontology of the IS artifact. The word security is simply the nominalized form of the predicate secure. In other words, security research is simply the examination of the property of being secure. While the Oxford dictionary defines secure as: “not subject to threat” or “protected against attack or other criminal activity”, it still leaves the question “what properties are threatened?”

In practice, information system researchers measure security threats in terms of their actual or potential impacts on the confidentiality, integrity, and availability (CIA) of an artifact (Parker 1998). These security concepts also apply to the physical world. Therefore, security is a second order property that is constructed from the first order properties of confidential, internally consistent (having integrity), and available. It is the inability of digital devices to maintain an internally consistent state that is problematic for realism.

Further examination of the secure property leads us to examine the essential properties of artifacts (those that must be present in order for an artifact to exist in its represented form) and accidental properties (attributes that do not alter an artifact’s classification based on their presence or absence) (Bennett 1969). Likewise, a closer examination of the intrinsic and extrinsic nature of the secure property is not clear-cut. Intrinsic properties are those which are present even when an object is duplicated, while extrinsic properties of an object can vary without changing the nature of the object itself (Lewis 1983). Finally, we must consider the materiality of the artifacts. More specifically, materiality consists of the arrangements or properties of the artifact that are important to users and that endure across space and time.
Tokens: Security at the IT Artifact Level

A researcher relying on critical or agential realism is concerned with a token’s properties, present in a specific space and time. I illustrate these concepts with a discussion of a safe (also known as a strongbox or coffer) in the physical world. A safe is a lockable storage device, used to secure objects (cash, other valuables) against unauthorized viewing, tampering, destruction or other loss of use. In order to provide this affordance, a safe must be lockable and have storage space; these are the essential properties of a safe, and every safe would have these two essential properties. Since, if these properties were altered, the artifact would no longer be a safe, these are also intrinsic properties. However, safes can be described in terms of many other properties, such as size, materials from which they are constructed, types of lock and unlocking mechanisms, and so on. These accidental properties vary from one type of safe to the next, yet each artifact remains a safe. The color, weight, and concealed nature of a safe are extrinsic properties which can be modified without altering the essential properties of the safe.

In the digital world, it is more difficult to identify items as simple as a safe. Although software that similarly provides the affordances of a safe exists (such as PGP desktop, TrueCrypt, or GPG Privacy Guard) this paper sacrifices some specificity in favor of a tangible and more popular artifact, a smartphone. While we may be tempted to only consider the digital component (software) of a smartphone and free ourselves from the physical manifestation of the device itself, this distinction is impossible. The digital artifact can only exist in a symbiotic relationship with the device—the hardware is useless without the digital software component and likewise the digital component cannot exist unless it is running on the device. This relationship is crucial to understanding the dynamic nature of the device type.

As with a physical safe, our digital device is capable of providing a user with lockable storage of digital objects (data), protecting these against unauthorized viewing, tampering, destruction or other loss of use. Similar to a physical safe, a smartphone has the essential and intrinsic properties of locking and storing data, while size and material properties remain accidental and extrinsic. While the environmental protection for the digital safe shifts from resistance to water from fire protection, the classification of this property is the same as the strongbox. Likewise, the color and weight of the device can be changed by adding protective covers or using different digital themes (colors schemes, backgrounds, etc.), but these properties do not alter how the device functions as a safe, so they remain accidental and extrinsic. However, unlike the mechanical classification and type of lock (accidental and intrinsic properties of the physical safe), the digital lock is essential to the digital safe and is extrinsic in nature. Without this property the device is simply a storage device, similar to a USB drive; however, if the device is duplicated, the lock can be altered (with a software upgrade) and still remain viable for protecting data. Therefore, unlike the physical world, the digital lock is essential and extrinsic in nature. Similarly, the unlocking mechanism in the digital world is accidental and extrinsic—it can be easily changed to start or stop using a passcode entered on the keypad, a camera for facial recognition, or fingerprint scanner. Table 1 below summarizes these properties of the digital and physical artifact:
Beyond Sociomaterial

<table>
<thead>
<tr>
<th>Artifact</th>
<th>Property</th>
<th>Essential/Accidental</th>
<th>Intrinsic/Extrinsic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safe</td>
<td>Locking</td>
<td>E</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Storage Space</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mechanical/Electric Lock</td>
<td>A</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Keypad/Combination/Key/Timing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Environmental Protection (Fire Resistance)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Size, Material</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Color, Weight, Hidden</td>
<td>A</td>
<td>E</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Locking Mechanism</td>
<td>E</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Data Storage</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Digital Lock</td>
<td>E</td>
<td>E</td>
</tr>
<tr>
<td></td>
<td>Environmental Protection (Water Resistance)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Size, Material</td>
<td>A</td>
<td>I</td>
</tr>
<tr>
<td></td>
<td>Unlocking Mechanism (keypad, fingerprint reader, camera)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Color, Weight</td>
<td>A</td>
<td>E</td>
</tr>
</tbody>
</table>

Table 1: Summary of the Properties of Tokens

Security Expands Properties of the Type

As discussed above, the realist generalizes the properties of a token to conceptualize types. In the physical world, in line with Quine and Quine (1987), the type of our safe is the set of all possible properties. In other words, our safe type has every property of the possible token safes. However, physical laws do not apply to software of which the digital world is comprised, because software properties can be boundlessly manipulated and instantly redefined. It is this emancipation from physical constraints, combined with the impact of security events that complicates the study of digital artifacts. Errors in coding logic are frequent, and may result in security vulnerabilities that allow a malicious agent to redefine the very nature of an artifact. For example, errors in authentication systems (such as ssh\(^1\) and telnet\(^3\)) used in digital artifacts are not uncommon and major releases of Apple’s iPhone (software versions 5.1\(^4\), 6.1\(^5\), 7.0\(^6,7\), 8.0\(^8\)) have contained errors that allowed users to bypass the lock on the device. Once a malicious user has bypassed the initial security mechanisms, they have the ability to view, alter, and delete the digital store. Attackers may also have the ability to surreptitiously and permanently alter the software running on a device\(^9\), thereby introducing new properties such as surveillance to our digital lockbox (Forristal 2013). When a new property is introduced, the digital safe can be used for a number of nefarious purposes such as track the user’s movements; take photos and videos; disclose to whom, when, and for how long the user communicates; and make copies of the data the user is trying to protect\(^10\). The reliance of a digital safe on the physical device on which it is stored means that charging cables and charging stations can also be used to alter the digital artifact to add new properties (Chumley 2013).

These unintended modifications become an issue when studying IT artifacts constructed from both digital and physical components. Because the properties of a digital artifact can be boundlessly manipulated in unpredicatable ways, we are forced to accept one of three possibilities with the digital type. A follower of Quine’s logic might argue that the digital type comprises of an infinite set of properties. While this approach may appeal to the likes of Schrödinger, for whom every possible future exists until it is observed (Schrödinger 1935), this notion is difficult to comprehend and also fails to provide any practical guidance to our ontology. Clearly the nominalist view can tempt us to believe there are no types in the digital

---

10 http://forensics.spreitzenbarth.de/android-malware/
Beyond Sociomaterial

We can resolve this discord by adopting a functionalist approach to define a security function. The social agency and the IT artifact are inputs to the function, the properties of the artifact help define the function, and the secure state (secure or insecure) is the output of the security function. Figure 1 illustrates this conceptual view:

![Figure 1: Functionalist View of Securing the IT Artifact](image)

**Functionalism**

Functionalism must be well understood, for a researcher to abandon materiality (the nature and properties of the IT artifact) and apply this ontology. A functionalist view of a safe (whether a physical safe or a digital safe) is not concerned with the arrangement of the properties of an artifact that are important to the user. Rather, the functionalist view is only concerned with how the arrangement of properties affect the resulting state. In other words, in our example, the functionalist is solely concerned with the state of being secure. In the physical world, a traveler may place his passport in a hotel safe. The traveler is probably not concerned with the color of the safe, its weight (as long as the safe cannot be easily removed), nor if the safe has a mechanical dial versus an electronic keypad. Physical safes vary; each hotel is likely to provide a different safe for the traveler to securely store valuables. The intent of the traveler is to protect his possessions from loss or damage (one input to the function); the safe (another input) is available to satisfy this intent. Both inputs to the function are influenced by the safe’s properties (as well as other factors accounted for in the function). The function results in a secure state or an unsecure one.

The user of our digital safe may prefer safes provided by a particular producer, but the specific encryption algorithms and methods used to compile and link software (how it is constructed) are likely not of great concern to most users, as long as they result in software that protects the user’s data. The software artifact can be replaced with another token, encryption algorithm, or other software components which offer the same affordances and result in the end state of security being satisfied (or not). There are various properties of the artifact that are just as useful for the end-user, and this is the concept of multiple realizability.

Multiple realizability causes a functionalist to ignore the nature of properties and instead focus on system inputs and outputs. Put mathematically, consider a function $f(x)$. The functionalist observes that when function $f(x)$ is applied to the number 6, the result is 36, and when the same function is applied to the number 7, the result is 49. The specific function may thus be $x^2$, $x(x)$, $x^3/x$, or a more complex algorithm, such as “for (1 to x): $x = x + x$” [add the number to itself, the same number of times as the number]. All of these expressions are mathematically equivalent and provide the same result regardless of the exact implementation.

If we revisit the radio telescope example to illustrate the distinction between agential realism and functionalism, the impact of this ontological change for an IS researcher becomes clear. An agential realist would be concerned with how the astronomer uses and makes sense of the audio/visual representation of radio frequencies. The functionalist would be concerned with the fact that the radio telescope allows a user the ability to detect phenomena; however, the functionalist is not specifically concerned with the device and its representation of extraterrestrial signals. For a functionalist, the type of an object is not
determined by its internal properties; it is determined by its *functional role*. An attacker may be able to alter the properties of a digital artifact; however, its functional role (even if broken) remains consistent between the user and the artifact.

This discussion may seem to imply that the IT artifact doesn’t matter, adding more tinder to the conflagration regarding the role of the artifact in research. However, the functionalist view does not contradict either materialism or dualism. The IT artifact is indeed a crucial input to the function, yet the artifact’s properties (or arrangement) do not matter to the functionalist. IS studies should be concerned with the function of the artifact, properties are part of the internal “black box” and should be atheoretical and uninteresting to the IS researcher. In fact, due to security issues in the digital world, the properties of the type are boundless and dynamic and therefore of limited theoretical use. An *agential functional* approach is compatible with sociomateriality but much easier to apply. The agential functional approach is an instantiation of functionalism where the artifact and the social are not mutually constructed; instead perceptions, intent of the agent, and the IT artifacts are inputs to a function, which results in an output state.

**Conclusion**

If the goal of social sciences is to understand and explain the associations between human and non-human elements, we must study both specifics and universals in order to make generalized theories. This is accomplished by the examination of tokens of digital artifacts and generalization to types. However, unlike artifacts in the physical world, the properties of digital components can fundamentally be altered by exploitation of security vulnerabilities to add or alter properties—unknown and undesired by the primary users of the devices. Therefore, if one holds a realist view of types in the physical world, their consideration of the digital artifact type must draw boundaries on how properties are defined. This limits the usefulness of the research. If we are only seeking to theoretically understand and explain with our theories, then such a boundary is clearly constrained to the past or present point in time.

However, when attempting to use theories to predict future outcomes, security vulnerabilities in the digital artifacts make it impossible to conceive the properties of a universal artifact. If the nature of the artifact and its properties are endlessly renegotiated, a realist must draw boundaries in their studies and assume the properties of the artifact will remain static in the future or will only change in predictable ways. An agential cut is only able to examine materialities at a specific point in time, and in a specific token context—any prediction is reduced to opinion of what agents may or may not construct.

For the realist, types span time and place, properties of the type that may be realized in the future are always present. Future properties are extended to the past resulting in unbounded possibilities. This infinite set of properties, in many ways, is equivalent to the nominalist view of a typeless world. However, the type for a functionalist is defined by its functional role instead of by its properties. This allows research to retain a type/token distinction necessary for generalized theories. For this reason, the *functionalist view* from the philosophy of the mind can be a useful approach to theorizing about the IT artifact. Perhaps, it is time to consider a move beyond sociomaterial and take an alternative approach to theorizing about the IT based on the philosophy of the mind’s functionalism—agential functionalism.
References


