THE ACCEPTABLE STATE: AN ANALYSIS OF THE CURRENT STATE OF ACCEPTABLE USE POLICIES IN ACADEMIC INSTITUTIONS

Complete Research

Jake Weidman, The Pennsylvania State University, State College, PA, jakeweidman@google.com
Jens Grossklags, Technical University of Munich, Munich, Germany, jens.grossklags@in.tum.de

Abstract

The Acceptable Use Policy has been a mainstay of organizational security for decades. These foundational policies were originally designed to detail sets of rules and requirements for users on an organizational network to follow while using a given network's resources, and often contained a series of restrictions dictating what users were not permitted to do. As organizational security models have progressed, newer policies, standards, and guidelines have been progressively introduced, and often contain similar, more specific requirements that users must follow when using an organizational network. Based on these developments, we ask the following: In the increasingly complex organizational security landscape, are Acceptable Use Policies still relevant?
In this study, we conduct a study utilizing 176 Acceptable Use Policies currently deployed at universities in the United States. Using a number of methods including a detailed coding of each policy, we present a summary on the current state of Acceptable Use Policies, as well as the university environment they exist in. We find that while Acceptable Use Policies are not relevant from a technical standpoint, they serve as a legal foundation to a university's security efforts, and as such could be improved upon in the modern organizational landscape.

Keywords: Policy Analysis, Acceptable Use Policy, Information Systems, Policy Management

1 Introduction

The modern organizational security landscape is increasingly complex, covering various threats and myriads of countermeasures. Large, public data breaches at companies such as Target, Yahoo, and others (Fitzgerald, 2012; McGrath, 2014) have continued to impact organizations and consumers. While the details of these breaches generally vary, intentional or unintentional employee actions are often at least partially blamed (Liginlal, Sim, and Khansa, 2009; Richardson, 2008), with employees being specifically targeted in instances such as phishing (Ohaya, 2006) and ransomware (Fimin, 2017) attacks. In defending against these types of data breaches, the primary means for an organization to manage its employees is via a set of rules and requirements that take the form of policies. This was reinforced by a recent study on cybercrime (Ponemon Institute, 2016) in which 4 of the 7 key takeaways/recommendations focused entirely on the *construction and implementation of strong technology and information policies*. This motivates an examination of the current state of organizational security practices and implementations to determine how these organizations are currently adapting to the technical and societal landscape of modern security. However, this task is easier said than done. Organizations readily identify and present public-facing policy as it pertains to consumer rights, in particular, regarding the use of consumer data. Analyses have been provided for documents including privacy policies (Jensen and Potts, 2004), End

User License Agreements (Grossklags and Good, 2007), and consumer-oriented fraud policies by banks (Becker et al., 2018), among others. However, (internal) corporate security policies, which guide the construction and implementation of technical systems, as well as mandate employee action, are often not publicly, or even upon request from academics, exposed to anyone who is not an employee of that organization. As a result, very few research studies regarding internal corporate security policies have been conducted and published (Kotulic and Guynes Clark, 2004).

In recent years, colleges and universities have become increasingly popular targets due to the increasing amount of intellectual property generated by these organizations (Bouchie, 2005; Siegel, Veugelers, and Wright, 2007). Prominent universities such as Stanford University (Hayward, 2013), UC Berkeley (Gilmore, 2015), and Cornell University (Bogel-Burroughs, 2017) have all suffered data breaches in the past several years, and reports have shown that upwards of 789 colleges and universities have suffered data breaches since 2005 in the United States alone (Privacy Rights Clearinghouse, 2017). Based on the number of degree-granting universities in the US as maintained by the US Department of Education, this indicates that at a minimum 17% of all U.S. universities have previously suffered some data breach - a non-trivial number (National Center for Education Statistics (NCES), 2016). In contrast to corporate organizations, academic institutions often do publicly share their internal policies regarding technology and user behavior on their networks. Similar to corporate organizations, academic institutions also employ and serve a large number of users in many cases (i.e., faculty, staff, students, third-party vendors), and also produce a large amount of valuable intellectual property. Therefore, we argue that academic institutions, including colleges and universities, are an apt choice to study the current state of technical policy to determine whether or not these institutions are doing enough to protect themselves, as well as their employees and students, from cyber-attacks.

Over the course of several decades, these technology and information policies have evolved from simple, short documents defining what the internet is and what its uses should be, to complex, technically-oriented document portfolios providing highly specific instructions defining user behavior on a network. While these technology and information policy documents have become increasingly complex, they all share a common origin: the Acceptable Use Policy. The Acceptable Use Policy, conceptually, is designed to manage employees' (and others') actions while using a given network. The *original* goal of these policies in most organizations was to encourage legal and productivity-focused actions, or limit potential actions that could be damaging to a particular organization. Over time, weaknesses of these Acceptable Use Policies were identified such as technological implementation shortcomings (Stewart, 2000), and thus different types of policies were constructed to fill these gaps (though Acceptable Use Policies were not removed). In this new, crowded policy space the question arises, what is the continuing role of the Acceptable Use Policy, and has this type of policy remained relevant?

2 Related Works

2.1 Modern Organizational Security Landscape

The modern organizational landscape, at least from a security policy perspective, has many layers, each with a different purpose. At the highest level of this system, policies exist to set the strategic direction, scope, and tone for an entire organization, and to drive the actions prescribed by all documents beneath them. Additionally, these policies should detail all contextually-relevant legal requirements an organization is required to follow and enforce. These policies are generally constructed by upper management, usually via a CISO or CIO, and should apply to an entire organization (Goodman, Straub, and Baskerville, 2016). Following the implementation of high-level policies, organizations often design a series of standards, which generally exist to provide more specific technical requirements that are mandatory for individual systems. These technical requirements, generally derived and inspired by elements of a higher-level policy, could include such items as forming strong passwords, detailing required encryption methods, or noting specific requirements for mobile device management, among many others (Von Solms, 1999).

Standards differ from policies in two key ways. The first deals specifically with intended target audiences. While policies are designed to be global documents that impact all members of an organization, standards often do not. Rather, specific sub-groups of the population are targeted, with different requirements directed at different groups. For example, an organization may have a security standard designed for system administrators, and another one designed for standard employees, both with drastically different requirements (Stanford University, n.d.). The second way that standards differ from policies is the highly explicit set of rules and instructions that must be followed by certain individuals. While policy documents note requirements at a high level, and often leave some rules open to interpretation (Yanow, 1995), standards ought to provide clear, concise lists of *exactly* what must be done by members of an organization.

The final series of documents contained within the modern organizational security landscape are those of practices, procedures, and guidelines. While policies are designed to set high-level goals, and standards are designed to explicitly state required technological concepts, practices, procedures, and guidelines (referred to as just guidelines henceforth) exist to provide means for all individuals within organizations to actually *implement* the required policies and standards (Bragg, 2002). To fully understand the difference between all three different document types, we provide the example of a password policy. At the highest level, perhaps in an information security policy, a statement loosely relating to passwords might be as follows: "All members of the University community must comply with secure and responsible administrative, technical, and physical practices." In this case, passwords may not even be explicitly mentioned as part of the policy. Rather, the term 'secure [...] practices' is used. Proceeding lower in the organizational document structure, a standard might note the following about passwords: "You should select a strong password and set your system up to require that password when you start the computer", or "Any default or vendor-supplied password must be changed to a non-default value." In these examples, passwords are clearly mentioned, and are referred to as a mandatory requirement. However, many standards still do not specifically describe how passwords should be constructed, hence the need for a guideline. An example of a guideline for passwords might be as follows: "A Strong Password should - Be at least 8 characters in length; Contain both upper and lowercase alphabetic characters (e.g. A-Z, a-z); Have at least one numerical character (e.g. 0-9); Have at least one special character (e.g. !@#$%&̂*()_-+=)."

As many of these newer organizational security documents have been implemented, it remains unclear if older policies, such as Acceptable Use Policies have been updated accordingly, or continue to be relevant as other high-level policies have been implemented such as information security policies. Likewise, as newer technologies often replace and negate the existence of older technologies, is the same true for high-level, older organizational policies such as the Acceptable Use Policy? In the following section, we detail the historical origin of the Acceptable Use Policy to understand its desired role in organizational systems.

2.2 Acceptable Use Policies

To counter ever-present security threats, and to better manage themselves, many organizations have spent significant time and effort to clearly define their internal structures and operations via a series of formal documents. At the highest level in this system, policies exist for two reasons: 1) to detail the required practices necessary to protect an organization from threats, and 2) to provide rules and other guidance to employees or members of an organization to direct their actions (Smith, 2015).

One of the original documents that sought to guide individuals in their use of technology on a network is the Acceptable Use Policy, also historically referred to as an Internet Acceptable Use Policy. In 1989, the National Science Foundation (NSF), a key entity in maintaining the internet, introduced a draft for what would be the one of the first Acceptable Use Policies for their NSFNET Backbone, a major underlying source of the internet at that time (Leiner et al., 1997; *The NSFNET Backbone Services Acceptable Use Policy* 1992). The original document contained only 3 sections with 11 total points which defined the general principle and reasoning behind the policy, as well as 7 specific acceptable uses, and 2 unacceptable

uses. The internet, at that time, was highly focused on research and education, and thus the only two 'forbidden' actions on the network were to conduct personal or private business, or to do anything for-profit. As the internet continued to evolve into the 1990s, this simple Acceptable Use Policy was often questioned, especially by those wishing to move their companies onto the internet (D. Wilson, 1993). It was often noted that it was unclear where the 'internet' itself ended, and the NSFNET Backbone began, ultimately leading to the creation of commercial networks that spawned the now-known internet. As more and more organizations began to connect to the internet and make their own private intranets, they (too) chose to adopt and create their own Acceptable Use Policies for their own organizations. Modern Acceptable Use Policies, similar to the original, can be described as primarily needing to fulfill three functions: 1) to educate users about behavior and activities considered to be harmful to an organization, 2) note that legal actions can be taken against those who violate determined acceptable behaviors, and 3) to protect the organization itself from any liabilities resulting from unacceptable computer use by those addressed by the policy (Laughton, 2008). These functions, while general, provide organizations with the means to protect themselves and their resources, at least from a policy perspective.

When organizations began to implement their own Acceptable Use Policies, many of them focused on improving the efficiency of their employees by reducing a practice called 'cyberloafing', or employees using organizational resources for personal use during business hours (Lim, 2002), in addition to reducing any illegal activities that employees could take part in such as online gambling, distributing copyrighted or inappropriate materials, and more (Blanchard and Henle, 2008). In this line of work, it was found that Acceptable Use Policies that were constructed with strict language, clear disciplinary actions, and a low tolerance mentality for violations provided a greater sense of 'fairness' for employees affected by these policies, and that instituting periodic monitoring (both in an Acceptable Use Policy and in practice) could reduce cyberloafing. However, research focused on cyberloafing soon began to find that some digressions could actually be beneficial to organizational goals, allowing employees to take short breaks to overcome stress, and to re-focus their attention on work-related tasks (Lim and Chen, 2012).

In reviewing the literature, this is a somewhat common pattern which we attempt to describe here. Initial research suggests changes or practices that should be implemented within these policies, to then be overruled or reconsidered at a later time (for example, the Lim papers on cyberloafing mentioned in the previous paragraph were separated by 10 years, and constitute two contrasting viewpoints on the same subject). Other research suggests rabbit-hole-type conundrums that prove difficult to solve. As an example, some research might suggest that strong policy enforcement and clearer language (Ward, Griffiths, and Whitmore, 2002) would be beneficial for enhancing employee policy compliance. Further research then implies that organizations that actively enforce their policies and, for example, limit personal use of organizational resources while working, drive down employee morale, and eventually productivity (Urbaczewski and Jessup, 2002). To counter this, later research then suggests that letting employees do the opposite of this, and thus backing off policy enforcement leads to greater employee morale and productivity (Oravec, 2002).

2.2.1 Beyond the textbook: Policies in Practice

Perhaps one of the largest shortcomings in Acceptable Use Policy literature is the prevalence of prescriptive Acceptable Use Policy papers, but the lack of research following up on whether these prescribed organizational practices were effective. A plethora of articles exists from the mid-1990s to early 2000s to advise the best practice or guidelines for constructing various Acceptable Use Policies (Gaskin, 1998; Palgi, 1996; Whitman, Townsend, and Aalberts, 2001). The content of these policy papers drives the aforementioned sections in this work, which adequately describe what should be included within these Acceptable Use Policies, and why. However, very limited work is sourceable which describes the inverse: the determination of what in-practice policies are actually incorporating, and thereby how effective they are. Two papers (published around 10 years ago) focused on the analysis of smaller sets of Acceptable Use and Information Security Policies, with generalized findings related to security, access management,

acceptable/unacceptable behavior, license compliance, roles & responsibilities, user monitoring, sanctions and project management with few generalizable findings (Doherty, Anastasakis, and Fulford, 2009, 2011). Though not focused on Acceptable Use Policies, previous ECIS work has also analyzed the content of a larger corpus of *information security policies* to perform a similar knowledge-gap evaluation of *in practice* policies, beyond existing prescriptive policy literature (Weidman and Grossklags, 2018). These works indicated that individual organizations implemented relatively distinct policy documents, and often seemed to follow no clear common policy templates in terms of policy construction (Weidman and Grossklags, 2018). Research also commented on the increasing complexity of organizational security policies, and questioned what the role of the Acceptable Use Policy might be in that scenario (Doherty, Anastasakis, and Fulford, 2011).

As such, the primary research gap that this paper aims to address is to provide insight as to how policies are implemented in reality, beyond the confines of prescriptive and contradictory literature. Through assessing these documents in practice, we argue that we are able to make inferences about the effectiveness of these policies, especially as they are situated in 2019 in a more crowded policy document landscape.

3 Methods

3.1 Selection and Pre-Processing of Acceptable Use Policies

Locating and selecting applicable Acceptable Use Policies was a multi-step process. To begin the selection, we first limited our search to universities contained in the Top 200 list as denoted by U.S. News (U.S. News, 2017), which sorts and ranks the top universities in the United States annually. For each university, we attempted to locate their respective Acceptable Use Policy, or similarly-themed document, to the best of our abilities. In some instances, we were either unable to find a comparable policy, or were prevented from downloading a given policy by access restrictions of university intranets.

In searching for the policies, we generally attempted to perform a Google search utilizing the name of a given university, accompanied by keywords such as 'acceptable use', 'appropriate use', or 'responsible use'[1]. If a given Acceptable Use Policy was located via this search mechanism, it was then read, cataloged, and downloaded by the researchers. In instances where a university's Acceptable Use Policy was not easily located, two general alternative techniques were employed. The first technique was to attempt to find a given university's Information Technology (IT) page and manually search it for links to technology policies enforced by that department, which often included the Acceptable Use Policy. In the event that a policy was still not discovered, the second technique required searching for a university's global policy page, and then searching the entire policy directory.

When locating Acceptable Use Policies using the second and third methods, we often encountered issues in locating 'Acceptable Use' policies based on a wide-ranging nomenclature. Thus, we attempted to locate any document that indicated by title, and by content, that it was effectively an 'Acceptable Use' policy. Such examples of this ultimately included 'Computer Use and Copyright Policy', 'Information Technology Users Privileges and Responsibilities', 'Technology Systems Usage Policy', 'Professional Standards and Business Conduct – Use of University Technological and Information Resources', 'Conditions of Use and Computing Ethics', or 'Computer Policy'. This list of alternatively-titled 'Acceptable Use' policies is not exhaustive; we found other variants in nomenclature as well. However, each of these documents was effectively designed to be an Acceptable Use Policy, as they each stipulated behaviors that were and were not permitted by users of a network.

If all three methods for searching for Acceptable Use Policies yielded no results, or if the university stored said policies within an intranet, that university was marked as either not having, or not permitting access to their Acceptable Use Policy. Using these data collection techniques, we ultimately identified

[1] Search terms such as 'responsible use' were added to the search mechanic after discovering it as nomenclature across several 'acceptable use'-type policies.

and downloaded 176 policies from 200 universities (88% success rate). These Acceptable Use Policies were collected between November 6-10, 2017, and were permanently archived by March of 2018 to preserve the state of the policies at that time. After downloading each policy, each was also converted to plaintext and cleaned (removal of special characters, unnecessary formatting etc.) as a preparation to perform automated text analysis on the policies themselves.

3.1.1 Statement on Selected Universities & Research Ethics

We would like to again formally note that we only identified and selected Acceptable Use Policies that met our selection criteria and were publicly available on university websites through our discovery process. We did not attempt to circumvent any organizational boundaries (such as intranet authentication mechanisms) or other security mechanisms to access these policies. Additionally, we do not intend to pass any judgment on a specific university's policy implementation as a result of this research. Any analysis or examples of university policy statements as part of this work are used only for demonstration purposes, and are not intended to cast any university in a negative or positive light. Rather, the goal of this work is to provide an overview of the Acceptable Use Policy space as a collective, not to focus on specific policy instances.

3.2 Coding of Acceptable Use Policies

A large portion of the analysis of this work stems from the coding of the 176 collected policies. In developing the coding schema, we evaluated previous studies and classical Acceptable Use Policy literature found in textbooks, with a final set of code items based on five key categories. The first of these categories is what we describe as Policy Management or Organizational Properties, which includes 7 sub-items including whether or not the policy clearly states an individual or entity responsible for the document itself, if it has an effective date, presents technical definitions, and more. These items are based on original internet Acceptable Use Policies, as well as more modern security policy analyses (Doherty, Anastasakis, and Fulford, 2011; Lichtenstein, 1996). As suggested by previous literature, it is noted that one of the key points of an Acceptable Use Policy should be to inform users about what kind of expectation for privacy they should have while using a network (Flowers and Rakes, 2000; Laughton, 2008). Thus, the second category we recorded was based on the concept of Privacy and/or User Monitoring.
The third category of measured items was focused on any concrete security technologies specifically detailed in a given policy including user account control, password requirements, anti-virus, and anti-malware requirements, as based on previous Acceptable Use Policy security literature (Laughton, 2008). Perhaps the most important category, i.e., the fourth category we measured, was based entirely on Network Behavior, or more specifically the sections of Acceptable Use Policies which detail what individuals are and are not permitted to do on a network. As this is primarily what these policies are supposed to focus on (Siau, Nah, and Teng, 2002), we measured 10 distinct items including email usage, harassment, and more. Lastly, we constructed a Legal category designed to capture any general legal items within the examined Acceptable Use Policies, as denoted by previous literature (Doherty, Anastasakis, and Fulford, 2011).

3.3 Analysis of Acceptable Use Policies

We continued our analysis by turning to language composition of each policy. First, similar to privacy policy studies (Mcdonald et al., 2009), we calculated the Flesch-Kincaid readability scores (W. Wilson, Rosenberg, and Hyatt, 1997) of all individual policies, accompanied by the word counts of each. We also conducted a cross-policy, text-based comparison of all collected policies to determine if there were any common phrases used across policies, or if policies tended to share content, themes, or similar language. This was done utilizing anti-plagiarism software, though we note that this analysis was conducted to track common or repeated phrases that might be found generally, and not to accuse any individual university of

copying or mimicking another's policy. Through this analysis, we were able to load all 176 universities into a full matrix analysis for similar text content, resulting in 30976 document comparisons.

4 Results

4.1 Acceptable Use Policies

4.1.1 Policy Management/Organizational Properties

Within the Policy Management coding category, we measured several items to determine how respective policies were managed by departments or individuals. The first of these measures was to determine how many of the policies clearly stated the entity or person who issued, or is responsible for their university's Acceptable Use Policy, thus declaring responsibility over this document. We found that 54.5% of the policies contained this information, indicating that 45.5% of policies did not contain any information about an author or authority figure. Often, for universities that did contain this information, a small table would be presented at the beginning or end of an Acceptable Use Policy indicating who the responsible party was, which was generally a CIO, CISO, or Vice President. Along a similar thread, we also captured whether a policy clearly stated who was affected by it. We found that 71.6% of the examined Acceptable Use Policies did contain this information. A common example of such a statement, as seen in Ball State University's policy, was: "This [acceptable use] policy applies to all students and employees, as well as all others who make use of Ball State University information technology resources and services."

The next several analysis items focused on policy implementation dates as well as the existence of a formal plan to update a policy regularly, based on the existence of a formal review date. When reviewing whether a policy had an implementation date, we chose to use the date for the most recent update we could find, in the event that we were able to view the original policy date as well as any proceeding updates. We found that 80.7% of the Acceptable Use Policies did contain an implementation date of some form. The most recently updated policy was Fordham University, on February 1, 2018, while the oldest policy we located was from the University of Nebraska, which indicated that it was last updated on March 1, 1999. The average most recent update date across all universities was July 25, 2013, indicating that, on average, the Acceptable Use Policies we examined were five years old. Concerning the existence of a policy 'next update' date, we found that only 10.2% of the policies contained this information. For those that did advertise a next update, we found that universities either provided an exact date that the policy would be reviewed, or would use some form of blanket statement indicating that the policy would be reviewed on an annual, or semi-annual basis.

We also investigated whether or not each Acceptable Use Policy contained a statement that a given policy was mandatory, and whether sanctions for violators were detailed as well. Of the policies we examined, we found that 47.2% of the universities had any form of statement asserting that the Acceptable Use Policy was required to be followed. One example of this was found via Illinois State University, which provided the following instructions: "An individual who uses ISU Information Technology Resources and Systems is responsible for compliance with this policy. Specific responsibilities include but are not limited to:[...]". Regarding the existence of sanctions for those who may violate an Acceptable Use Policy, 68.2% of the universities provided such information. What this indicates, in some ways, is that the existence of sanctions may be intended to imply that such a document is mandatory, as more universities provided information about sanctions compared to those who stated whether the policy was mandatory.

The last policy management item we measured was whether or not the collected Acceptable Use Policies provided any sort of definitions for any technical items contained within the policies. To that end, we found that 32.4% of the universities provided this information. An example of some common definitions provided can be seen in the policy of the Florida Institute of Technology, who provided definitions for topics such as E-Commerce, Hacked, Spam, and more.

4.1.2 Privacy/User Monitoring

As stated in related work (Holmes, 2003), a critical component of any Acceptable Use Policy should be that organizations detail user data monitoring practices on their network (if applicable), and why this monitoring is taking place. To that end, we found that 64.8% of the universities we analyzed contained any type of information about data monitoring practices. In one example, the university not only stated information regarding data monitoring, but also provided some reasons (virus scanning, etc.) to illustrate why such monitoring might occur. This practice of detailing reasons for data monitoring was carried out by 44.3% of the universities. In turn, this means that 20.5% of the universities indicated that the users of their network may be monitored, but provided no reasonable explanation of why. For those universities that did provide justifications, the detailed reasons often related to the need to ensure system integrity, and to comply with state or federal laws, including public requests for information under the Freedom of Information Act.

4.1.3 Security

Beyond informing individuals about general behaviors that are or are not permitted, we posited that some Acceptable Use Policies would also contain rules and regulations regarding several common security technologies. Thus, we sought to determine whether some basic technical rules regarding passwords, anti-virus software, or more, might be present within these policies. For the most part, we found that this was not the case. Beginning with anti-virus requirements, we found that only 15.3% of the universities had any mandatory requirements to use anti-virus on university-affiliated or connected systems. For anti-malware, this number was even lower at 1.7%. Considering specific password requirements, only 9.7% of the policies provided such requirements, often stating fairly standard password rules (no dictionary words, longer than 6 characters, requirement for a special character, etc.). Lastly, only 12.5% of the policies specified anything *specific* about user account control, which in the case of this work, refers to a university's attempts to provide rules for users to manage their accounts (password rotation/protection, username security, etc.). While nothing specific was mentioned, however, nearly every Acceptable Use Policy we examined had some kind of statement noting that users should aim to protect their account from false access, and should not give anyone their credentials.

4.1.4 Network Behavior

The measured category of Network Behavior contained ten total items relating to actions that may be explicitly permitted or prohibited on a network. To begin, the item 'Work-related use of systems' was based on the concept that in more traditional organizations, Acceptable Use Policies often had statements indicating that organizational equipment or networks were to be used for work-related tasks, and could not be used for any personal tasks (Young, 2010). We found that only 9.7% of the policies provided any statement that their resources were to be used for work-related purposes only, supporting the current existing literature that some dual use may be productivity-enhancing. One example of such a statement came from the New Jersey Institute of Technology: "Cyber resources are to be used for university sanctioned activities consistent with the mission of NJIT. University sanctioned use includes, but is not limited to: instruction; completion of academic and administrative assignments; academic research and scholarly activities; [...]".

The second item we measured was related to email; specifically, if the Acceptable Use Policies made any statements about potentially inappropriate email usage including spam, chain letters etc. Slightly over half of the universities (51.7%) had any sort of policy requirements addressing this issue. New School noted the following prohibitions, among others, of email use via a bulleted list: sending unsolicited e-mail messages, assuming the identity of another user via email, soliciting e-mail for the sake of harassment, or creating/forwarding chain letters. Beyond email, Acceptable Use Policies should state other actions that are prohibited, even if these may be deemed to be somewhat 'common sense'. Such an example of this is

having a rule that indicates that individuals using a network are not permitted to gain access to any system they are not authorized for, especially by means of hacking or cracking a security system. We found that 68.8% of the policies provided such a statement, or series of statements. Hofstra University noted this as a point on an unordered list of unauthorized actions: "Hacking or attempting to circumvent security on another computer [is prohibited]". Similar to hacking-related policy terms, many universities also noted further prohibitions including the act of distributing viruses or malware on a network, or physically damaging equipment or network resources. 41.5% of the universities had such (brief) statements including, "[It is not permitted to] Transmit computer viruses or malicious/destructive code of any description", as seen at Northeastern University. Regarding the protection of physical computing resources, 24.4% of the policies made a statement about the necessary protection of these resources, with an example from Arizona State University noting: "Conduct leading to the damage of ASU electronic information/data, computing/networking equipment, and resources is prohibited."

While protecting physical resources is a high priority, protecting other users is one as well. To capture this aspect, we determined how many universities had any sort of policy concept explicitly centered around protecting other members of a network from each other. In this case, we found that only 10.8% of the policies had such a statement, such as Hofstra University, which noted: "I will respect the privacy and reasonable preferences of other users (both at Hofstra and elsewhere on all connected networks), including the privacy of their accounts and data." We do note that while only 10.8% of the universities provided a statement specifically about doing anything negative towards other users on a network, it is possible that other aspects of the policy could be interpreted to mean the same thing. Specifically, policy concepts which attempt to limit harassment or the breaking into of accounts of other computing resources could be considered to be statements also designed to protect users from each other.

In addition to protecting other users and resources on the network, universities and other organizations need mechanisms to protect themselves from external threats, in this case specifically related to lawsuits attributed to the illegal downloading or uploading of videos, music, pornography, and more. We found that 23.9% of the sampled universities provided any statements prohibiting illegal downloads, while 21.0% provided a similar statement regarding illegal file uploading. Johns Hopkins University noted the following about illegal downloads and uploads (referred to here as distribution): "An illegal action on the Johns Hopkins network includes, but is not limited to: Unauthorized distribution or downloading of copyrighted material, including: Music, Movies, Television Shows, Computer Software [...]."

The final item that we measured within the Security category was that of commercial and political activity on a network. We found that 67.0% of the universities provided such a statement, barring students, faculty, and others from using network resources for commercial gains (such as hosting a for-profit website), or for political purposes (such as distributing political emails, using university printers for the creation of political materials, etc.).

4.1.5 Legal Issues

The final section we examined via our corpus of Acceptable Use Policies was that of Legal Issues, or more specifically details of copyright protection and appropriate use, and state or federal law compliance. Beginning with copyright rules, we found that 69.9% of the policies provided some type of statement or statements regarding the use, distribution, and required protection of copyrighted material. Tulane University referenced copyright in the scope of unauthorized distributions of copyrighted material: "Unauthorized distribution of copyrighted material is a violation of federal law. In accordance with the Digital Millennium Copyright Act, the University, once notified of alleged copyright violations, will disconnect from the network the server or computer of the individual(s) involved. The individual who is distributing the copyrighted materials is responsible for any copyright infringement." Meanwhile, other universities focused on the ownership and use of such materials in classroom settings or otherwise, such as Kent state which noted: "A university member who stores or distributes copyrighted material must be the copyright holder or have the permission of the copyright holder as required under law. This

includes duplication of audiotapes, videotapes, photographs, illustrations, computer software, and all other information for educational use or any other purpose."
Regarding state and federal law statements and, therefore requirements, we found that this item category was found with the greatest frequency, with 80.1% of the universities providing statements or sections about legal compliance. While many universities made mentions of such laws via simple statements indicating that all state and federal laws should be followed (without any details on what laws those might be), other universities provided more specific examples including specific state of federal statues.

4.2 Readability Analysis

After completing the coding portion of the Acceptable Use Policy analysis, we implemented a series of quantitative methods as a means to further examine the policies. At first, we generated Flesch Reading Ease scores, as well as word count for each policy. When running these tests, we found that the mean readability score of these policies was 19.96 (SD=9.76). Any Flesch Reading Ease score that is below a 30.0 is intended for a college graduate, and is inherently difficult to read. In total, only 12.3% of the Acceptable Use Policies had a readability score of 30 or higher. Andrews University maintained the highest readability score at 46.27, while Suffolk University had the lowest score at -13.35 (or, effectively 0.0). The average length of these Acceptable Use Policies was 1793.18 words (SD=1156.59). The shortest policy was Stanford University at 221 words, while the longest was Fordham University with 6730 words.

4.3 Acceptable Use Policy Cross-Comparison

The final analysis we conducted on the dataset of Acceptable Use Policies was to perform a cross-document policy comparison to determine how similar, based on exact language, the policies were to each other. Identifying any differences or commonalities between these documents can potentially provide insights about core elements of these policies, and may reveal which components of policies might be deemed to be the most critical across organizations. Results are based on the total number of policy document comparisons (30976).
We found that very few policies shared a substantial amount of information. Only 264 policy document comparisons (0.85%) contained more than 10% of similar content to each other, and only 68 document comparisons (0.22%) were 20% similar to each other. Examples of similar text that would be included in this sample would generally be short, common phrases such as "other relevant University polices." In other cases, longer phrases were found such as the following: "Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under the University's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records[...]." For documents that were more similar to each other (20% or greater), several entire document phrases were often similar to each other, with the addition or subtraction of a small number of words in a given phrase. An example of this can be seen in the text below taken from two policies that were found to be more than 25% related to each other (differences between the policies are italicized; normal-faced text indicates this was the same across both policies):

> While the university does not routinely monitor individual usage of its information resources, the normal operation and maintenance of (*these resources//the University's computing resources*) require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the (*provision//rendition*) of service [...].

Where these similarities occur, it is not initially clear why some aspects of these policies are shared content. It could be that universities share information or are open to sharing policy content, or perhaps these universities have shared a similar CISO or policy writer(s). Additionally, it could be that this text is taken from a popular policy textbook, or some other generally applicable template. Although it is unclear how these similarities occur, it is still worth noting that this applied to only a very small number of policy

documents that we examined in this dataset, and was not very common. We consider this small amount of overlap surprising given the long history of Acceptable Use Policies.

5 Discussion

5.1 Prevalence and Timeliness of Acceptable Use Policies

An initial goal of this paper was to determine how relevant Acceptable Use Policies were within the current organizational security policy landscape. Based on this high-level goal, we find several takeaways. The first is that these Acceptable Use Policies are still in use at a very large number of universities (88% of our sample size). What varied more, however, was how frequently these policies were updated by their respective universities. While some universities had seemingly updated their Acceptable Use Policies as recently as February 2018, others were not so modern, and on average we found that the Acceptable Use Policies in our dataset were $\sim$5 years old. Further, 12.5% of the policies we analyzed were at least 10 years old, with the oldest policy being dated as March 1, 1999. Although logic might dictate that the newer a given technology-related policy is (given the evolving threat landscape), the better, we pose the question: are less current Acceptable Use Policies actually a troubling issue?

Traditional information security management literature notes that it is critical that policies contain information regarding their original implementation date, as well as any dates on which revisions took place (Whitman and Mattord, 2013). However, this literature typically does not make the point that it is absolutely necessary for policies to be reviewed annually, though many non-academic sources such as blogs or business websites may suggest this (Gasior, 2017; Williams, 2018). The primary reason behind frequently updating policies is to ensure compliance with various new laws (Whitman and Mattord, 2013), though additional arguments could be made about ensuring technological terminology remains relevant, among others. In many of the older Acceptable Use Policies we examined, we often encountered descriptions of devices or nefarious cyber-behavior that we had not been exposed to in some time. Examples of this included device-based references towards Palm Pilots (PDAs), or towards more action-based terms such as 'email bombing' or 'auto dialing'. Although these terminologies are not entirely relevant in 2018, we make the argument that there is no technical or reasonable need to modify or remove such terms. The reasoning behind this is that while most individuals are no longer using PDAs, an incident may still occur in which someone might try to connect such a device to a given network. If this device was not 'covered' by a policy, an individual may be able to use the argument that they were free to behave on a network as they wished. Essentially, we argue that policies in this sense should be additive, not necessarily subtractive. As many of the older laws are still in practice to protect against older-style crimes or behaviors, so too should at least some older provisions in Acceptable Use Policies.

While policies may be able to reference older technologies without consequence, these documents must be able to evolve with newer legal requirements dictated by state and federal governments. Though not as relevant in the United States, nearly all organizations in Europe have had to update most of their technology policies due to the enactment of the General Data Protection Regulation (GDPR) (*Regulation (EU) 2016/679 (General Data Protection Regulation)* 2018). Organizations in the United States must similarly comply with the Electronic Communications Privacy Act (Federal level) or the California Electronic Communications Privacy Act (state level), as examples. Considering that a large number of Acceptable Use Policies we examined contained information specifically noting compliance and enforcement of certain state and federal laws, it is clear that Acceptable Use Policies should be checked and updated frequently to ensure they are fully accurate and up-to-date with applicable laws.

To answer the question originally posed at the beginning of this section, we argue that while Acceptable Use Policies may not need to be completely up-to-date in terms of technical definitions or references, these policies should be checked and updated regularly to ensure compliance with all state and federal laws. Older polices, especially those over 5 years old, risk relaying false information that may be followed by

individuals on a network. It is the responsibility of organizations to ensure these policies remain relevant, and performing annual reviews and revisions is a desirable practice.

5.2 Acceptable Use Policies in Practice

The second key objective of this work was to determine how Acceptable Use Policies currently function in-practice at a large number of organizations, and in this case, universities. To summarize the role of the modern Acceptable Use Policy in a single sentence, it would be as follows: The Acceptable Use Policy serves as a foundational document to dictate what users are and are not permitted to do on a given organizational network, with an emphasis on non-technical aspects of behavior and legal compliance. This definition is in line with previous, though limited, literature on the subject of Acceptable Use Policies (Arnesen and Weis, 2007; Van Roekel, Berry, and Bell, 2004). What we can more clearly show in this work, however, is what a majority of these permitted and non-permitted user actions are, and note them in an accessible manner. We begin by denoting what Acceptable Use Policies are not; namely, they are not technical documents. Whereas other policy documents, such as information security policies, might formally outline technical specifications (such as password requirements), Acceptable Use Policies only sparely mention such aspects, if at all. Beyond content, we also found that the policies we examined were generally difficult to read, with an average readability score of 19.96 (college graduate level or higher). Considering that organizations such as universities employ many types of individuals, and also cater to recent highschool graduates, these unfavorable readability levels could potentially hinder the ability of some to effectively read and comprehend these documents.

When determining the most commonly occurring items within this corpus of Acceptable Use Policies, we found that these documents were predominately focused on describing actions that were permitted and not permitted for individuals using a given university's network. In a majority of cases, this took the form of a list, or series of lists, which detailed *permissible* actions one could take while on a network. This would include things like using email 'appropriately', or to 'have respect for others'. In other instances, the approach was more reductive, with some policies detailing lists of things that were *not permitted* on a network such as 'do not waste university resources', or 'disrupting access to systems'. When running various comparisons between the two approaches, we found no clear advantage, indicating that both methods have some merit to relay policy information. In terms of the similar content that was discussed across policies, the most common topics were those of state and federal legal compliance, copyright, personal business use of a network, and organizational monitoring of data. While each of these topics is worthy of inclusion in an Acceptable Use Policy, these topics are fairly obligatory, with perhaps the exception of organizational monitoring, though this has been the subject of prior work (Stephen and Petropoulakis, 2007). Considering that a majority of the policies we examined were significantly different from each other, both in terms of text-based comparisons and policy coding, the fact that these three items occurred most commonly across all policies is telling.

Based on these findings, we note that the modern Acceptable Use Policy seems to be primarily focused on ensuring proper legal compliance, both from a governmental regulation and copyright law standpoint, as well as indicating how a given organization might monitor users on their network. Many Acceptable Use Policies also contain additional information, which detail actions that users are able to, and not able to, do while using a given network. These actions generally focus on the protection of individual user accounts, proper use of email and other technology resources, and the restriction of network resources to conduct business for personal financial gain, among others. While each of these provided actions may be important to a given organization, based on the lack of commonality between policies, they may not be important to all organizations. This also stresses the point that organizations are heavily focused on individual differences when constructing their Acceptable Use Policies, and thus it is difficult to give generic recommendations regarding what should be included in a standard Acceptable Use Policy. However, through the results section of this paper, we provide a series of examples taken from a wide

sample of policies, which could serve as inspiration for those wishing to have examples of common Acceptable Use Policy terms.

5.3 The Role of Acceptable Use Policies Moving Forward

During our collection of policies from universities, we found that a major university had actually retired the policy from service in the latter-half of 2017. With the average examined Acceptable Use Policy being ∼5 years old, and with not very many clearly definable attributes, it is worth considering what the future role of the Acceptable Use Policy is. With so many different policy documents, standards, and guidelines all included within the organizational security space, it is potentially easy to overlook older, foundational policies such as the Acceptable Use Policy. However, when considering the alternative of removing the Acceptable Use Policy, it is not initially clear where the topics contained in such policies would be relocated to. In many ways, the Acceptable Use Policy is like an old law. It contains somewhat complex legal jargon, is difficult to read, and uses somewhat outdated language at times. However, in lieu of a suitable modern replacement, these older policies, like older laws, need to remain in place to provide a foundational policy that was often the original basis of many organizations' information security plans. The Acceptable Use Policy, while simplistic in its design, provides a critical series of instructions that dictate how users are supposed to behave on an organizational network, and what the consequences are for violating these norms. In that sense, the Acceptable Use Policy is still an important part of the organizational security paradigm, and should continue to be for the foreseeable future.

6 Conclusion

In this work, we presented a study of 176 Acceptable Use Policies used at universities in the United States to determine the modern design and applicability of these well-known, but not well-studied policy documents. Through detailed coding and automated analyses, we find that while Acceptable Use Policies are still very much in use by many organizations, their content is difficult to generalize. Commonalities across policy documents were mostly reflected in the areas of legal compliance and copyright control, with other elements appearing depending on organizational differences. We do find that Acceptable Use Policies are not intended to be technical, and are rather designed to quite generally direct user behavior on an organizational network. When analyzing the policies in an automated manner, we find that these policies are inherently difficult to read and are written in a very analytical manner. Lastly, we find that a majority of Acceptable Use Policies share very little content with each other in terms of a direct text comparison, with many policies sharing less that 5% of similar content.

While Acceptable Use Policies are somewhat dated in terms of their introduction and implementation, many organizations still update and utilize these policies regularly. Without an appropriate substitute, Acceptable Use Policies continue to be needed to guide user behavior on organizational networks. Although many of the policies that we examined lacked a common core set of features, we posit that our examination of these documents produced an understanding of the current state of Acceptable Use Policies and their contents in practice. We anticipate that this study further contributes to the knowledge and understanding of policies and procedures that exist within the organizational security landscape, and serves as a reference to those looking to enhance their own organizational security policy framework.

Acknowledgments

We want to thank the anonymous reviewers and editors for their constructive comments and feedback. This research was partially supported by the German Institute for Trust and Safety on the Internet (DIVSI).

References

Arnesen, D. and W. Weis (2007). "Developing an effective company policy for employee Internet and email use." *Journal of Organizational Culture, Communications and Conflict* 11 (2), 53–65.

Becker, I., A. Hutchings, R. Abu-Salma, R. Anderson, N. Bohm, S. J. Murdoch, M. A. Sasse, and G. Stringhini (2018). "International comparison of bank fraud reimbursement: Customer perceptions and contractual terms." *Journal of Cybersecurity* 3 (2), 109–125.

Blanchard, A. and C. Henle (2008). "Correlates of different forms of cyberloafing: The role of norms and external locus of control." *Computers in Human Behavior* 24 (3), 1067–1084.

Bogel-Burroughs, N. (2017). "Hacker 'Rasputin' breaches Cornell, attempts to sell access." *The Cornell Daily Sun*.

Bouchie, A. (2005). "Survey reveals US university licensing up, startup formation down." *Nature Biotechnology* 23 (2), 261–262.

Bragg, R. (2002). *CISSP Certification: Training Guide*. Que Publishing.

Doherty, N., L. Anastasakis, and H. Fulford (2009). "The information security policy unpacked: A critical study of the content of university policies." *International Journal of Information Management* 29 (6), 449–457.

— (2011). "Reinforcing the security of corporate information resources: A critical review of the role of the acceptable use policy." *International Journal of Information Management* 31 (3), 201–209.

Fimin, M. (2017). "Are employees part of the ransomware problem?" *Computer Fraud & Security* 2017 (8), 15–17.

Fitzgerald, D. (2012). "Yahoo passwords stolen in latest data breach." *The Wall Street Journal*.

Flowers, B. and G. Rakes (2000). "Analyses of acceptable use policies regarding the Internet in selected K–12 schools." *Journal of Research on Computing in Education* 32 (3), 351–365.

Gasior, M. (2017). *Why It Is Important to Review Policies and Procedures*. URL: `https://www.powerdms.com/blog/why-it-is-important-to-review-policies-and-procedures/`.

Gaskin, J. (1998). "Internet acceptable usage policies." *Information Systems Management* 15 (2), 20–25.

Gilmore, J. (2015). "Campus announces data breach." *Berkeley News, University of California at Berkeley*.

Goodman, S., D. Straub, and R. Baskerville (2016). *Information Security: Policy, Processes, and Practices*. Routledge.

Grossklags, J. and N. Good (2007). "Empirical studies on software notices to inform policy makers and usability designers." In: *International Conference on Financial Cryptography and Data Security*. Springer, pp. 341–355.

Hayward, B. (2013). "Investigating apparent IT breach, Stanford urges users to update passwords." *Stanford University*.

Holmes, J. (2003). "Formulating an effective computer use policy." *Information Strategy: The Executive's Journal* 20 (1), 26–32.

Jensen, C. and C. Potts (2004). "Privacy policies as decision-making tools: An evaluation of online privacy notices." In: *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, pp. 471–478.

Kotulic, A. and J. Guynes Clark (2004). "Why there aren't more information security research studies." *Information & Management* 41 (5), 597–607.

Laughton, P. (2008). "Hierarchical analysis of acceptable use policies." *South African Journal of Information Management* 10 (4), 2–6.

Leiner, B., V. Cerf, D. Clark, R. Kahn, L. Kleinrock, D. Lynch, J. Postel, L. Roberts, and S. Wolff (1997). "The past and future history of the Internet." *Communications of the ACM* 40 (2), 102–108.

Lichtenstein, S. (1996). "Internet acceptable usage policy." *Computer Audit Update* 1996 (12), 10–21.

Liginlal, D., I. Sim, and L. Khansa (2009). "How significant is human error as a cause of privacy breaches? An empirical study and a framework for error management." *Computers and Security* 28 (3-4), 215–228.

Lim, V. (2002). "The IT way of loafing on the job: Cyberloafing, neutralizing and organizational justice." *Journal of Organizational Behavior* 23 (5), 675–694.

Lim, V. and D. Chen (2012). "Cyberloafing at the workplace: Gain or drain on work?" *Behaviour & Information Technology* 31 (4), 343–353.

Mcdonald, A., R. Reeder, P. G. Kelley, and L. Cranor (2009). "A comparative study of online privacy policies and formats." In: *Proceedings of the International Privacy Enhancing Technologies Symposium*. Springer, pp. 37–55.

McGrath, M. (2014). "Target data breach spilled info on as many as 70 million customers." *Forbes.com*.

National Center for Education Statistics (NCES) (2016). *Digest of Education Statistics*.

Ohaya, C. (2006). "Managing phishing threats in an organization." In: *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*. ACM, pp. 159–161.

Oravec, J. (2002). "Constructive approaches to Internet recreation in the workplace." *Communications of the ACM* 45 (1), 60–63.

Palgi, R. (1996). "Rules of the road: Why you need an acceptable use policy." *School Library Journal* 42 (8), 32–33.

Ponemon Institute (2016). *Cost of Cyber Crime Study & the Risk of Business Innovation*.

Privacy Rights Clearinghouse (2017). *Data Breaches*. Continuously updated database. Last accessed on June 7, 2017. URL: `https://www.privacyrights.org/data-breaches`.

Regulation (EU) 2016/679 (General Data Protection Regulation) (2018). URL: `https://www.eugdpr.org/`.

Richardson, R. (2008). *CSI Computer Crime and Security Survey*. Computer Security Institute. eprint: `arXiv:1208.5721`.

Siau, K., F. Nah, and L. Teng (2002). "Acceptable Internet use policy." *Communications of the ACM* 45 (1), 75–79.

Siegel, D., R. Veugelers, and M. Wright (2007). "Technology transfer offices and commercialization of university intellectual property: Performance and policy implications." *Oxford Review of Economic Policy* 23 (4), 640–660.

Smith, R. (2015). *Elementary Information Security*. Jones & Bartlett Publishers.

Stanford University (n.d.). *Minimum Security Standards*. University IT. URL: `https://uit.stanford.edu/guide/securitystandards`.

Stephen, B. and L. Petropoulakis (2007). "The design and implementation of an agent-based framework for acceptable usage policy monitoring and enforcement." *Journal of Network and Computer Applications* 30 (2), 445–465.

Stewart, F. (2000). "Internet acceptable use policies: Navigating the management, legal, and technical issues." *Information Systems Security* 9 (3), 1–7.

The NSFNET Backbone Services Acceptable Use Policy (1992).

Urbaczewski, A. and L. Jessup (2002). "Does electronic monitoring of employee Internet usage work?" *Communications of the ACM* 45 (1), 80–83.

U.S. News (2017). *National University Rankings*. U.S. News Rankings.

Van Roekel, J., M. Berry, and M. Bell (2004). "Acceptable use policy." In: *Internet and Personal Computing Fads*. CRC Press, pp. 19–20.

Von Solms, R. (1999). "Information security management: Why standards are important." *Information Management & Computer Security* 7 (1), 50–58.

Ward, J., P. Griffiths, and P. Whitmore (2002). *Strategic Planning for Information Systems*. Wiley Chichester.

Weidman, J. and J. Grossklags (2018). "What's In Your Policy? An Analysis of the Current State of Information Security Policies in Academic Institutions." *Proceedings of ECIS 2018, European Conference on Information Systems*.

Whitman, M. and H. Mattord (2013). *Management of Information Security*. Nelson Education.

Whitman, M., A. Townsend, and R. Aalberts (2001). "Information systems security and the need for policy." In: *Information Security Management: Global Challenges in the New Millennium*. IGI Global, pp. 9–18.

Williams, M. (2018). "Ask an expert: How often should our IT policies be reviewed and updated?" *IT Strategy, Services and Support for London and Beyond*. URL: `https://www.pensar.co.uk/blog/it-policies-reviewed-and-updated`.

Wilson, D. (1993). "'Acceptable use policy' on Internet prompts confusion over commercial activities." *The Chronicle of Higher Education*.

Wilson, W., L. Rosenberg, and L. Hyatt (1997). "Automated analysis of requirement specifications." In: *Proceedings of the 19th International Conference on Software Engineering*. ACM, pp. 161–171.

Yanow, D. (1995). "Practices of policy interpretation." *Policy Sciences* 28 (2), 111–126.

Young, K. (2010). "Policies and procedures to manage employee Internet abuse." *Computers in Human Behavior* 26 (6), 1467–1471.