Received 16 August 2017
Accepted 16 August 2017

Top secret from the bottom up

Message classifications by non-state organizations and their members

Craig R. Scott and SoeYoon Choi
Department of Communication, Rutgers University, New Brunswick, New Jersey, USA

Abstract

Purpose – The emerging area of message classification is one of growing relevance to a wide range of organizational communicators as a variety of non-state organizations and their members increasingly use and misuse various terms to restrict their communication. This includes formal classifications for data security, financial/knowledge management, human resources, and other functions as well as those used informally by organizational members. Especially in a data-rich environment where our word-processing programs, e-mail tools, and other technologies afford us opportunities to engage in classification, a wide range of people at all organizational levels may serve as custodians of their own data and thus have the ability (as well as perhaps the need) to classify messages in various ways. The purpose of this paper is to describe key classification terms ranging from those found in government (e.g. top secret, confidential) to those in the private sector (e.g. business use only, trademarked) to an even wider set of terms used informally by organizational members (e.g. personal, preliminary). The growing use of message classifications will likely create various challenges and opportunities for organizations, their members, and the broader public/society. A set of future research questions is offered for corporate communication researchers and practitioners, who are well positioned to examine this emerging phenomenon.
Design/methodology/approach – This paper draws on existing literature related to the growing use of message classifications to offer a list of classification terms and an agenda for future research.
Findings – This work describes key classification terms ranging from those found in government (e.g. top secret, confidential) to those in the private sector (e.g. business use only, trademarked) to an even wider set of terms used informally by organizational members (e.g. personal, preliminary). This expanded notion of classification will likely create various challenges and opportunities for organizations, their members, and the broader public/society.
Originality/value – The emerging area of message classification is one of growing relevance to a wide range of organizational communicators as a variety of non-state organizations and their members increasingly use and misuse various terms to restrict their communication. A set of future research questions is offered for corporate communication researchers and practitioners, who are well positioned to examine this emerging phenomenon.

Keywords Private, Confidential, Message classification, Non-state organizations, Restrictions, Top secret
Paper type Research paper

Government organizations have long been concerned with document classification schemes to protect state secrets by distinguishing them with labels such as secret and top secret. Some estimates suggest that this classified universe is five to ten times larger than all the literature in our libraries (Galison, 2004). However, this classified universe may be even larger if we look beyond nation states and start to consider other organizations and organizational members that also engage in these efforts (e.g. organizations dealing with sensitive information as well as those interacting directly with government agencies). Beyond that, organizations and their members in any sort of communication-intensive field are already beginning to use message classifications that serve to restrict communication in key ways. In their e-mail signatures, their documents, and even in conversations with various stakeholders they may label messages as private, for internal use only, personal, unofficial, or as any one of dozens of other terms that attempt to restrict communication. In an era where data are so pervasive (and so regularly subject to unwelcome disclosures), surveillance capabilities are growing, and

A previous version of this paper was presented at the Annual Conference of the European Group for Organization Studies, Copenhagen, Denmark (2017, July).

Corporate Communications: An International Journal
Vol. 22 No. 4, 2017
pp. 556-561

1356-3289
DOI 10.1108/CCIJ-08-2017-0072

privacy has become increasingly contested amid calls for transparency, various non-state organizations and their members are increasingly likely to (mis)use and encounter such classification efforts. Thus, this emerging area of message classification is one of growing relevance to a wide range of organizational communicators.

Beyond the state: classifications by other organizations and their members

Most government classification systems are designed to protect state secrets or at least to balance risks of disclosing such secrets against benefits of information access. For example, the USA currently uses four distinctions based on the damage that would be done if information was revealed (Lowenthal, 2017). Top secret is for information whose unauthorized disclosure could be expected to cause exceptionally grave damage to national security. Secret is for disclosures causing serious damage. Confidential is for disclosures that could be expected to cause damage to national security. More recently, the USA added a sensitive but unclassified distinction.

It is not difficult to imagine how similar classification practices could start to be used by other bureaucracies/organizations also. Indeed, some of the earliest writings about secrecy actually come from sociologists such as Weber (1946), whose work on bureaucracy suggests that timidity and inertia lead to an exaggerated tendency toward secrecy in these organizational forms (see Blank, 2009). Vaughn (2009) argues that secrecy is built into the very structure of organizations. More recently, Costas and Grey (2016) have argued that despite the difficulty of keeping secrets in an age of openness, secrecy continues to play a key role in organizations to protect trade secrets, proprietary products, intellectual property, and even state secrets as well as to facilitate noncompete and non-disclosure agreements. Trade secrets, which derive independent economic value by not being known or readily ascertainable to others who might benefit from such a disclosure (Hannah, 2005), are relatively familiar as a type of organizational secret. Another "key regulatory mechanism in formal secrecy is control over documents (whether physical or electronic), for instance, in the form of data protection laws" (Costas and Grey, 2016, pp. 76-77). However, beyond trade secrets and data/information security, other forms of restricted messages are not as well understood nor as uniformly applied across organizations.

"Within military and intelligence organizations, the classification of documents on the basis of ascending hierarchies of access (e.g. 'secret,' 'top secret') is commonplace, and the same terminology is sometimes employed within commercial settings" (Costas and Grey, 2016, p. 77); but, there are notable differences as well. For example, corporate security lacks some of the extreme penalties associated with government classification; furthermore, most companies rarely need a top secret classification. Instead, data classification and information security policies have suggested designations such as these: business use only or internal (unauthorized disclosure not expected to seriously affect organization) and confidential (disclosures would adversely affect organization; Rodgers, 2012); sensitive (data that will do the most damage to the organization should it be disclosed), confidential (might be less restrictive within the organization but might cause damage if disclosed), private (might not cause company damage but needs to be kept private for other reasons – such as laws related to human resources data), and proprietary (data disclosed outside a company only on a limited basis that contains information that could reduce a company's competitive advantage; Bragg, 2002); as well as non-disclosure agreement (NDA) confidential (should only be viewed by those who have an NDA), employee confidential (e.g. restricted to specific groups of management or boards), and private (for concealing identifying information; Landwehr, 2007). Others coming from more of a financial or knowledge management perspective have suggested classifications such as confidential (substantial threat to financial viability), restricted (could cause financial loss or loss of earning potential) and protect (which is similar but more about creating an unfair advantage; Cobb, 2009); or sensitive, confidential, and/or private (Clobridge, 2016). Of course, to that we could add terms coming from certain other professions/fields that may

influence how organizations have to restrict information (e.g. privileged, sealed, copyrighted, and trademarked). Thus, a range of formal classifications exist for use by non-state organizations – though the exact meaning of frequently used terms can vary across organizations and may differ from typical use in state-based formal classification schemes. Additionally, just as government has people designated to do classification (e.g. original classifiers), certain organizations have formal roles tasked to make these determinations (e.g. data security manager, privacy compliance official, human resources specialist, and perhaps even chief communication officer).

As important as such official classifications may be for data security, financial/knowledge management, human resources, and other functions, they overlook what we find to be a much less developed aspect of restrictive terminology use: those used by organizational members more informally. Especially in this data-rich environment where our word-processing programs, e-mail tools, and other technologies afford us opportunities to engage in classification, a wide range of people at all organizational levels may serve as custodians of their own data and thus have the ability (as well as perhaps the need) to classify that material in various ways. A consequence of all this is that we as organizational members and consumers/customers are increasingly confronted with a potentially confusing array of message classifications (with intended and unintended outcomes).

Key classification terms

These classifications serve a restricting function in that they limit what is in a message, how official or final it is, to whom a message is intended/unintended, with whom it might be shared, when a message may be sent/received, etc. The focus here is on messages because the restrictions are not only relevant to written documents but can also refer to oral exchanges and various digital forms. These restrictions may be within the content itself (e.g. a printed report depicted internally as private; an-in person negotiation described as unofficial) or proximate to the content (an e-mail subject line announcing the message is not for distribution; a word-processing document with a draft watermark on it). Users may even label messages with the strategy used to conceal them (e.g. encrypted, password-protected).

Table I provides examples of many of these terms. Clearly some are used by state organizations, by non-state entities, and by organizational members. Certainly, organizational members do label messages as confidential, private, official, classified, sensitive, and even trademarked. The degree of consistency or accuracy with which members employ such classifications is unclear – though experts have claimed that terms such as security, secrecy, confidentiality, and privacy are often used interchangeably (McClelland and Thomas, 2002) and that ideas such as privacy and secrecy are easily confused (Solove, 2002). Some organizational members may describe some of their exchanges as confidential or private. Some may claim copyright or trademark on phrases or presentation documents (regardless of whether they actually have secured such rights) and may describe the content of some exchanges as about proprietary information or as being privileged communication (regardless of any legal or business definitions of these terms). Such efforts may be on the rise as organizational members attempt to better protect their own privacy and lay claim to their own intellectual property.

In other cases, members may informally use terms that correspond closely but not identically to the more formal ones in state and non-state organizations. For example, a message labeled high risk may denote the sensitive and consequential nature of the content. A message labeled as censored is likely one where certain information has been edited out or removed before it was made available to certain audiences. We may instruct others to do not copy or not for distribution to limit who gets information and how widely it is shared. Communication professionals may be especially familiar with the need to embargo certain messages that are not to be shared until a certain time (e.g. after a press release has been sent);

State/government organizations – formal	*Other potentially restrictive terms – informal (in addition to all formal terms)*
Top Secret	Personal
Highly Secret	Draft
Secret	Preliminary
Confidential	Limited
Sensitive	(Un)edited
Restricted	Unofficial
For XX Eyes Only	Unauthorized
Need to Know	Void
Official	Invalid
Classified	Banned
Redacted	Forbidden
Protected	Blocked
Others primarily in non-state organizations – formal	Locked
Not for Distribution	Secured
Private	Reserved
Business Use Only	Censored
Internal or Internal Use Only	Embargoed
Non-disclosure	Do not Copy
Employee Confidential	Off the Record
Proprietary	High Risk
Privileged	Recalled/retracted
Sealed	Original
Trademarked	Exclusive
Copyrighted	Encrypted
	Password-protected

Table I.
Message classification: examples of potentially restrictive terms

individual organizational members can also label messages as embargoed to discourage sharing until a later point in time or actually use document and e-mail features to avoid sending messages or making them unreadable until a certain date. Even in interactions not involving journalists, individuals may discuss information off the record to indicate this is not to be shared and/or they are not to be associated with the comments.

Other terms of restriction are more specialized or more informally and selectively used by organizational members. For example, an organizational member may label a file personal to signal to others that such messages are not for others and to deter seeking such information. Organizational member may also use draft or preliminary on a report to indicate something is not ready to be shared because it is not in its final form. These terms and others like them (e.g. limited, edited) may also help to protect an author from critique by noting this is a first attempt. In other instances, organizational members may label messages as unauthorized or unofficial. These messages may not be finalized in some official sense (e.g. an unofficial notification of an award as we await approvals); but often they are finished – with these restrictive labels suggesting that a person is not acting in their official capacity or that the information being shared does not necessarily reflect the broader views of the employer.

Less commonly, we may find individuals labeling a document or other set of messages as invalid, banned, forbidden, etc. Again, these terms connote a level of secrecy and a desire to restrict the availability of certain information through labels denying access or discrediting the content. Related terms such as locked, secured, blocked, reserved, etc. also suggest restrictions in access somewhat generically (in that we may not know who is blocked or from whom such messages are being kept – but clearly the message is not intended for widespread public view). Labels that describe messages as password-protected or encrypted would fit here as well. We may even use certain e-mail or document sharing programs to recall messages (physically removing them from one's inbox or marking them as having been

recalled and thus not to be shared). For rather different purposes, a message may be labeled original or exclusive to help designate certain works as being special and/or belonging to the message sender.

Future directions

The formal use of these terms in state organizations – though not void of debates about what actually should be classified as secret, top secret, etc. – is highly prescribed and regulated in many ways. Some non-state organizations have also developed guidelines for their use of message classifications. But, especially as we start to consider informal organizational member usage of such terms, a series of questions begins to emerge relevant to organizational communication scholars and practitioners. How much variation exists in the use and intended meaning of such terms, especially across organizations? How is the informal use of classifications (re)constructing our more formal uses and understandings of these terms? What legal standing do members have when using such terms informally? What is the discursive force of such labels? How are such classifications reacted to by various stakeholders? How uniformly are these restrictive terms understood by those various audiences?

A different set of questions emerges related to motivations for these classifications and other influences on classification. What motivates individuals to restrict and classify messages? How strategic vs mindless are such choices? What are the individual and relational characteristics that influence message restrictions? What organizational and broader industry factors influence individual classification decisions? To what extent are such choices usefully understood as attempts to gain or retain power? How is message classification understood as face-saving or face-threatening? How do considerations of message audience factor into these decisions?

There are also costs and benefits of any efforts to classify – and this applies to informal efforts on the part of organizational members also. This consideration of message classification advantages and disadvantages raises more questions. For example, what are the material and social costs of classification efforts for organizations, their members, and the communities in which they operate? What are the dangers of more widespread use of message classifications by organizational members? What are the dangers of potentially limiting such informal efforts? What are the benefits linked to message restriction efforts? How is the cost-benefit of increased classification and restriction assessed in an era of visibility and transparency? What makes for appropriate message classification that stakeholders find socially acceptable? What qualities are associated with effective classification efforts that meet individual and/or organizational goals?

Although message classification guidelines relevant to organizations and their members do exist (see Landwehr, 2009; McClelland and Thomas, 2002; Rodgers, 2012), a number of questions remain. Even existing theory related to communication privacy (Petronio, 2002) and anonymity (Rains and Scott, 2007) does more to suggest possibilities than prescribe solutions. What technologies should organizations provide that afford members the ability to engage in this classification? How standardized should formal classification schemes in organizations be – and should efforts be made to provide some structure to more informal efforts? How do we increase literacy about classification so that it can be done more competently? How should various communication parties negotiate boundaries when it comes to restricted communication? How do we better consider the role of various message audiences (intended, unintended, and excluded) as they attempt to reduce the uncertainty often associated with restricted messages? What sort of classifications and restrictions do various audiences find more and less acceptable or more and less difficult to challenge?

In an era where a wide range of organizations – and especially a growing number of organizational members – are increasingly classifying messages with restrictive terms, it is essential that organizational scholars examine this more closely. We see this trend as

neither good nor bad – but believe it will continue to create various challenges and opportunities for organizations, their members, and the broader public/society. Corporate communication researchers and practitioners are well positioned to begin examining this emerging phenomenon.

References

Blank, L. (2009), "Two schools for secrecy: defining secrecy from the works of Max Weber, Georg Simmel, Edward Shils, and Sissela Bok", in Maret, S.L. and Goldman, J. (Eds), *Government Secrecy: Classic and Contemporary Readings*, Libraries Unlimited, Westport, CT, pp. 59-68.

Bragg, R. (2002), "Classifying data", in Bragg, R. (Eds), *CISSP Training Guide*, Pearson IT Certification, pp. 218-221, available at: www.pearsonitcertification.com/articles/article.aspx?p=30287&seqNum=9 (accessed January 6, 2017).

Clobridge, A. (2016), "Open knowledge versus knowledge management", available at: www.nxtbook.com/nxtbooks/onlinesearcher/20160304/index.php#/74 (accessed January 6, 2017).

Cobb, M. (2009), "How to apply government data classification standards to your company", ComputerWeekly, available at: www.computerweekly.com/news/1355736/How-to-apply-government-data-classification-standards-to-your-company (accessed May 6, 2009).

Costas, J. and Grey, C. (2016), *Secrecy at Work: The Hidden Architecture of Organizational Life*, Stanford University, Stanford, CA.

Galison, P. (2004), "Removing knowledge", *Critical Inquiry*, Vol. 31 No. 1, pp. 229-243.

Hannah, D.R. (2005), "Should I keep a secret? The effects of trade secret protection procedures on employees' obligations to protect trade secrets", *Organization Science*, Vol. 16 No. 1, pp. 71-84.

Landwehr, J. (2007), "Information classification-what does 'confidential' mean?", November 15, available at: http://blogs.adobe.com/security/2007/11/information_classification_wha.html

Landwehr, J. (2009), "Document security: minding your documents", S C Media, February 5, available at: www.scmagazine.com/document-security-minding-your-documents/article/555423/ (accessed January 6, 2017).

Lowenthal, M.M. (2017), *Intelligence: From Secrets to Policy*, 7th ed., Sage, London.

McClelland, R. and Thomas, V. (2002), "Confidentiality and security of clinical information in mental health practice", *Advances in Psychiatric Treatment*, Vol. 8 No. 4, pp. 291-296.

Petronio, S. (2002), *Boundaries of Privacy: Dialectics of Disclosure*, State University of New York Press, Albany, NY.

Rains, S.A. and Scott, C.R. (2007), "To identify or not to identify: a theoretical model of receiver responses to anonymous communication'", *Communication Theory*, Vol. 17 No. 1, pp. 61-91.

Rodgers, C. (2012), "Data classification: why is it important for information security?", April 3, available at: www.securestate.com/blog/2012/04/03/data-classification-why-is-it-important-for-information-security

Solove, D.J. (2002), "Conceptualizing privacy", *California Law Review*, Vol. 90 No. 4, pp. 1087-1155.

Vaughn, D. (2009), "Structural secrecy", in Maret, S.L. and Goldman, J. (Eds), *Government Secrecy: Classic and Contemporary Readings*, Libraries Unlimited, Westport, CT, pp. 460-470.

Weber, M. (1946), *From Max Weber: Essays in Sociology* (Trans by H. Gerth), Oxford University Press, Oxford.

Corresponding author
Craig R. Scott can be contacted at: crscott@rutgers.edu