Page Proof Instructions and Queries

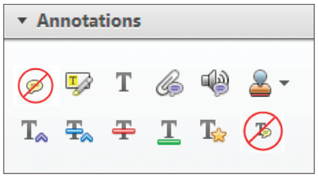
Journal Title: BIR

Article Number: 651781

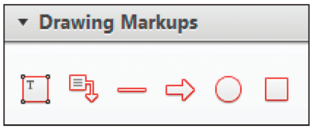
Greetings, and thank you for publishing with SAGE. We have prepared this page proof for your review. Please respond to each of the below queries by digitally marking this PDF using Adobe Reader.

Click "Comment" in the upper right corner of Adobe Reader to access the mark-up tools as follows:

For textual edits, please use the "Annotations" tools. Please refrain from using the two tools crossed out below, as data loss can occur when using these tools.



For formatting requests, questions, or other complicated changes, please insert a comment using "Drawing Markups."



Detailed annotation guidelines can be viewed at: http://www.sagepub.com/repository/binaries/pdfs/AnnotationGuidelines.pdf

Adobe Reader can be downloaded (free) at: http://www.adobe.com/products/reader.html.

No.	Query
	Please confirm that all author information, including names, affiliations, sequence, and contact details, is correct.
	Please review the entire document for typographical errors, mathematical errors, and any other necessary corrections; check headings, tables, and figures.
	Please confirm that the Funding and Conflict of Interest statements are accurate.
	Please note that this proof represents your final opportunity to review your article prior to publication, so please do send all of your changes now.
AQ: 1	Please provide complete reference details for Reference Court of Justice of the European Union, 2014.
AQ: 2	Please provide complete reference details for Reference Floridi, 2014.

BIR

Business Information Review
1–4
© The Author(s) 2016
Reprints and permission:
sagepub.co.uk/journalsPermissions.nav
DOI: 10.1177/0266382116651781
bir.sagepub.com
SAGE

Social media, risk and information governance

David Haynes
City University London, London

Abstract
The use of social media by organizations forms an important component of the information landscape. However, social media governance is often overlooked even though its use needs to be managed in order to avoid some of its pitfalls. Risk management is one way of developing a strategy for regulating the use of social media by employees, and this article argues that it forms the basis for an effective information governance framework.

Keywords
General Data Protection Regulation (GDPR), information governance, information security, risk, social media

Introduction

Social media are widely used by companies to promote their products and services. They play a valuable role in internal staff communications and as fora for customer feedback. Use of social media by employees may be work-related or for private use. In both instances some kind of policy or set of guidelines is needed. By social media, we mean web-based applications where users provide personal profiles and generate their own content. Within social media, social networking services (SNSs) have attracted particular attention because of the personal nature of the information that is provided and the attendant risks associated with this.

Social media such as Facebook, Twitter and Instagram are widely used by organizations and their employees. This may range from corporate pages on social media that consumers can follow to active campaigns and viral marketing initiatives to generate interest in a product or service. It can also be a general presence to convey the values and brand of an organization – particularly if they are targeted at younger people. SNSs generate massive amounts of exploitable consumer data. It provides a revenue model that drives the digital economy. SNS providers depend on the sale of user behaviour data to advertisers to generate income. Users benefit by gaining access to these services free at the point of use. In return, their personal data and transactional data are made available to digital advertising agencies who sell those on to third parties for targeted marketing. Social media use has an impact on consumer-oriented businesses and public services that pay for advertising and promotion, representing both risks and opportunities.

Risks

There are risks associated with the use of any technology or service and social media use is no exception. The challenge arises because there has until recently been very little analysis of this type of risk. We can make a distinction between risks to individuals and corporate risks. Part of the problem is one of education. If social networking interactions are seen as being as private as a conversation with a friend or a small group of friends, it gives licence for unconstrained exchanges. The difference between this and casual conversations is that social media provide a permanent record of what was exchanged. It is a semi-public forum where it is notoriously difficult to control the spread of information beyond its originally intended audience.

In a survey of stakeholders in the UK, in addition to the harms associated with privacy breaches, the following risks of social media to employers were identified (Haynes and Robinson, 2015: 103):

> Many of the risks to employers of using SNSs in the workplace are not related to access to personal data. They include issues such as: time wasting, security breaches, copyright and libel where staff members post inappropriate materials on an SNS site during work hours or on a site with a strong presence by or association with the employer.

Corresponding author:
David Haynes.
Email: dhaynes@aspiresquared.co.uk

This preliminary list can be expanded to include the following risks to organizations as a result of social media use by employees or customers:

- Reputational damage resulting from negative comments about the organization posted on social media.
- Breach of confidentiality through inadvertent or deliberate release of sensitive information.
- Data breach caused by releasing access codes or passwords.
- Regulatory non-compliance, such as data protection breaches that could lead to substantial fines and/or loss of reputation. Industry-specific non-compliance could lead to suspension of trading licence.
- Danger to individual employees by revealing sensitive personal data about health, domestic arrangements or location.
- Libellous statements posted on social media that can leave the host organization open to being sued.
- Technical exposure through weak firewalls could provide a route into sensitive IT systems or information.
- Fraud perpetuated as a result of information revealed on social media.
- Loss of opportunity (by not using social media).

Response to risk

Information governance is an important part of the information security framework. With the increasing recognition of the value of big data, organizations are beginning to devote significant resources to information management and information governance.

One response to these risks is to forbid the use of social media by employees at work or even at home. Preventing private use of social media by employees while not at work is questionable and difficult to police. Some organizations monitor the private use of social media by their employees to ensure compliance with organizational values. Where necessary sanctions can be applied to employees for inappropriate use of social media that exposes the organization to risks such as reputational damage, although no such control exists for customers short of going to court. More nuanced responses can be found in the social media policies of organizations, which have been made accessible via links from the Social Media Policies database (Boudreaux, 2015).

A snapshot of 12 social media policies examined for this article provided a useful indication of the perceived risks of social media use and some guidelines for staff behaviour. Two of the policies were generic and provide a template for members of the Chartered Institute of Public Relations (CIPR, 2013) and one for UK government departments (Cabinet Office, 2014).

An overview of the social media policies of some UK-based organizations representing news, security, government and retail products and services, suggested wide recognition of the value of social media. Many policies actively encourage staff to use social media technology. Some employers such as the British Broadcasting Corporation make a distinction between private use and official use of social media. The majority of policies stipulated that any postings that identify the employer should be professional and compliant with the organization's ethos. Many policies also provide helpful style guidelines that suggest informal, first person, open and transparent postings that are short, relevant and interesting.

Concerns focused on legality, compliance and safety. Employees were mostly required to put in a disclaimer about representing personal views and had some kind of procedure in place for checking content prior to publication. Legal issues such as intellectual property rights of others, defamation and breach personal privacy were mentioned. Compliance with industry or government standards was a requirement in many instances and data protection was regularly mentioned in this content. Safety and security were other concerns. Revealing sensitive operational information about the organization or technical information that would allow access to systems was highlighted. Employees were also made aware of the dangers to themselves and other employees if personal data is published on social media. This is particularly important in sensitive areas such as security services and the health services where patient confidentiality is emphasized.

The following messages can be gleaned from social media policies that were examined:

- Use of social media is a valuable tool and channel for internal staff communications, reaching out to customers and stakeholders and for raising the public profile of the organization.
- Private use of social media that identifies the employer should reflect the organization's values.
- Do show your enthusiasm for your organization and its products and services.
- Do reach out to the public and encourage interaction.
- Do be open and transparent. For instance if you have a vested interest in a product that you are promoting, say so.
- Respect individual differences and different opinions and do not use social media to vilify others (not even competitor organizations as this may leave you open to libel action).
- Respect intellectual property rights.
- Do not air unsubstantiated claims, accusations or rumours or anything potentially libellous.
- Do not reveal sensitive operational, personal or technical information via social media.

- Do no use social media for criticisms, suggested improvements or for whistle-blowing. There are other, more appropriate channels for doing so.

It would be foolhardy to have no guidelines on social media use. Inclusion in staff handbooks and as part of staff induction is a start. However, the culture of the organization is particularly important. Respect for other staff and for customers engenders an environment where disparaging comments are not considered acceptable – they are not part of the 'norms' of the organization. It could be argued that employees have a contractual obligation to protect the reputation of their employers. Social media are not an appropriate avenue for 'whistle-blowing', for instance. Properly managed corporate social media facilities may be an appropriate way of letting off steam – a kind of digital suggestions box. There might even be opportunities for sentiment analysis so that managers can identify concerns at an early stage before they become major problems. The kind of sentiment analysis used for Tweets could be applied to internal social media as well – especially for larger corporations with a lot of traffic on social media.

Information governance is an important part of an information security strategy. An information governance policy that does not allow for social media has a major gap.

A couple of policies refer to monitoring use of social media and this raises concerns about privacy. The Human Rights Act (UK Parliament, 1998) asserts 'Everyone has the right to respect for his private and family life, his home and his correspondence'. However, a recent court case that came to the European Court of Justice upheld the right of an employer to monitor employees' personal email communications at work. This has implications for employees throughout Europe and could extend to monitoring use of social media in the workplace.

The debate about regulating access to personal data has moved beyond privacy considerations. This demands a wider approach than relying on legislation alone. The Data Protection Directive of 1995 is the main legislation that governs use of personal data in the European Union (EU). Although it is Europe-wide and has been incorporated into national legislation (such as the UK's Data Protection Act 1998), its application to non-European companies has been problematic. Companies like Facebook and Google that are headquartered in the United States have tried to claim that they are exempt from EU legislation. Attempts to patch this up through the EU-US Safe Harbor agreement fell apart in 2015 when the European Court of Justice ruled that it was invalid as because of US security agencies' past record of seizing personal data from US companies. This has been replaced by the EU-US Privacy Shield, which also offers limited protection to European citizens (Haynes, 2016).

From a company point of view, lack of consistent rules across Europe is a problem. National interpretation of the Directive varies considerably. Germany is perceived as being very rigorous about enforcement, while the UK and Ireland are both regarded is 'hands off' or even lax by European standards. The new General Data Protection Regulation (GDPR) is intended to overcome this problem, by having a single Regulation across Europe rather than a directive enacted into in the national legislation. The authorities in each country will still be responsible for enforcement and public education about data protection.

A third problem with legislation is its lack of flexibility. Although the current Directive is based on principles rather than prescriptive, a lot of the detail and subsequent directives have been very technology-specific. As user behaviour evolves and new services are developed, legislation is in danger of lagging behind. Controversy about the 'right to be forgotten' is an example of legislation (and its enforcement) being out of step with current practice and market behaviour. In May 2014, the European Court of Justice upheld the decision of the Spanish court on an individual's right to be forgotten in the *Google Spain SL, Google Inc. v. AEPD, Mario Costeja Gonzaĺez* case (Court of Justice of the European Union, 2014). It forced Google Europe to remove links to an article that a Spanish lawyer found damaging to his reputation and, although true, irrelevant to his current situation. Despite the link being to a published newspaper announcement, which was itself a matter of public record, Google could not point to that article when a search was done on the lawyer's name. Google Europe responded by introducing a process to allow individuals to apply to have links to damaging references removed from search results. Not surprisingly a lot of requests came from convicted criminals and politicians who wanted to disconnect their names from online records of their past views or activities. For this and a number of other resources, there is a question about the enforceability of the right to be forgotten is unenforceable (Floridi, 2014; Haynes, 2014; Powles and Singh, 2014).

General Data Protection Regulation

This brings us to the GDPR, the wording of which was finalized in April 2016. The GDPR makes a number of provisions as well as beefing up the enforcement regime and the maximum penalties that would apply across Europe. The GDPR is due to be implemented 2 years after formal publication in the *Official Journal of the European Community*. It makes a number of new provisions.

The right to be forgotten described above is one of the main changes to the current legislation. Another new requirement is the obligation for organizations to report data breaches and to notify data protection authorities. There are also potentially unlimited fines for the most serious breaches of the regulation.

The GDPR will have an impact on non-European organizations if they operate within the EU, such as US organizations that are currently registered under the EU-US Privacy Shield arrangements.

Conclusion

Active management of social media use is essential to address some of the risks that organizations face such as reputational damage, legal liability for intellectual property breaches and security exposure. An important part of the response to these is to embed social media procedures in the information governance strategy. In the future, the GDPR will provide a focus for information governance strategies in the lead up to its implementation in 2018. Policies offer an advantage to companies because they often directly address the types of risk that the company is concerned about. They are also easy to understand and they provide a clear statement of intent. However, policies alone are not sufficient for maintaining the risks associated with social media use. Staff training and culture change are also required to ensure that the guidelines are followed. It's about teaching people traffic sense rather than banning cars because they are potentially dangerous.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

References

Boudreaux C (2015) *Social Media Policy Database*. Available at: http://socialmediagovernance.com/policies/ (accessed 21 April 2016).

Cabinet Office (2014) *Social Media Guidance for Civil Servants*. Available at: https://www.gov.uk/government/publications/social-media-guidance-for-civil-servants (accessed 21 April 2016).

CIPR (2013) *Social Media Best Practice Guide*, p. 27. Available at: http://www.cipr.co.uk/sites/default/files/CIPRSocialMediaGuidelines2013.pdf (accessed 21 April 2016).

Court of Justice of the European Union (2014) *Google Spain SL, Google Inc. v. Agencia Española de Proteccio´n de Datos (AEPD)*, Mario Costeja González. AQ1

Floridi L (2014) Google ethics adviser: the law needs bold ideas to address the digital age. *The Guardian*. AQ2

Haynes D (2014) Forget the Right to be Forgotten, Other Means Exist. *The Conversation*. Available at: http://theconversation.com/forget-the-right-to-be-forgotten-other-means-exist-29117 (accessed 21 July 2014).

Haynes D (2016) Privacy shield replaces safe harbour, but only the name has changed. *The Conversation*. Available at: https://theconversation.com/privacy-shield-replaces-safe-harbour-but-only-the-name-has-changed-54189 (accessed 22 February 2016).

Haynes D, Robinson L (2015) Defining user risk in social networking services. *Aslib Journal of Information Management* 67(1): 94–115.

Powles J, Singh J (2014) Academic commentary: google spain. *Cambridge Code*. Available at: http://www.cambridge-code.org/googlespain (accessed 21 July 2014).

UK Parliament (1998) *Human Rights Act*. London: The Stationery Office.

Author biography

David Haynes is a visiting lecturer at City University London where he teaches information management and policy on the #citylis course. He has been involved in information research and consultancy for over 30 years and recently completed a PhD at City University on 'Risk, Regulation and Access to Personal Data on Online Social Networking Services'. He is currently preparing the second edition of his book 'Metadata for Information Management and Retrieval' due out late 2016. He teaches a module on metadata and information taxonomies at the Centre for Archives and Information Studies at the University of Dundee. He is a fellow of CILIP and a member of the British Computer Society. As an active project manager, he is an advanced MSP practitioner and has a BCS Certificate in Data Protection.