Client Alert

18 February 2015

Top 5 Legal Issues You Need to Consider When Implementing an Enterprise Social Network

By Susan McLean and Mercedes Samavi

The clue is in the names – Jive, Chatter, Yammer. Enterprise social networks (ESNs) are designed to help employees communicate and share information and ideas. ESNs have been around for a number of years, but are becoming increasingly common in the mainstream corporate environment as individuals and organisations have grown more comfortable using social media as a business tool. In addition, with the rise in remote and mobile working, companies increasingly recognise the value of a more connected workforce.

The potential benefits of an effective ESN are clear. They are platforms that are designed to build relationships, streamline communication, reduce hierarchy and break down silos, promote collaboration and innovation, and instil a sense of community across organisations that are often distant – whether through geography, structure, or otherwise. The biggest challenge with ESNs, as with any business tool, is adoption by employees. Of course, ESNs also pose certain legal and regulatory challenges and organisations need to address a number of key issues when launching an ESN.

WHAT IS AN ESN?

An enterprise social network (ESN) is typically an enterprise-grade, third party, private social media platform designed for use by employees. Examples of third party platforms include Microsoft's Yammer, Saleforce's Chatter, Jive, and the recently-announced Facebook at Work. ESNs tend to offer a variety of different features including real-time chat feeds, document sharing, management and collaboration, and community networks. Many, but not all, are cloud-based solutions. However, although the third party ESNs may be the best known, ESNs can also be bespoke platforms or apps built in-house to meet the needs of an organisation's workforce (*e.g.*, the Barclays mobile app MySite, Heathrow's app for operations staff, etc.).

KEY ISSUES

1. Access Control

Deciding who gets access to your ESN is critical. Typically, a third party ESN will be accessible by anyone who has a corporate e-mail address. However, practically speaking, this could include individuals who are not employees, *e.g.*, contractors based on site. Giving such individuals access to the ESN may not be appropriate, particularly if it could trigger an increased risk that such contractors are considered employees. In addition, companies may want to invite third parties – for example, clients or consultants – to have access to certain areas of an ESN. Even within the employee population, there may be sections of the ESN that should only be available to certain employees or departments within the business, *e.g.*, Legal or HR. In each case, when deciding who

has access to your ESN, you will need to take into account appropriate legal and compliance issues in relation to the protection of confidential or privileged information, intellectual property rights, and personal data.

2. Social Media Policy

Social media, by its nature, induces spontaneous and real-time reactions from its users. Occasionally this may result in ill-judged contributions on the ESN, which will not only reflect badly on the user, but could adversely impact the organisation. Accordingly, it's important to put in place an appropriate social media policy. A company's existing social media policy that's primarily concerned with the use of external social networks may not appropriately cover an ESN. Accordingly, organisations should consider creating a social media policy specific to the ESN.

The policy should make clear what conduct is and is not acceptable, *e.g.*, no disclosure of confidential or sensitive information to employees or users who are not authorized to view that information. The policy should also make clear the forms of disciplinary action that may be taken in the event of a breach.

In addition to the policy, it's vital that users are provided with adequate training on the use of the ESN and compliance with the policy. However, it's also important to take a common sense approach. If the policy is too long, complicated or restrictive, the chances are that people will simply ignore it (and you could come unstuck if the policy is subject to a legal challenge). To help ensure that users understand the policy, be creative; perhaps create a slide show or video to accompany your policy.

In addition to implementing a policy, organisations will need to monitor the ESN and put in place appropriate procedures to deal with breaches of policy. Again, a pragmatic, light-touch approach is recommended, because too much unnecessary interference may stifle adoption. In addition, organisations will need to ensure that any such monitoring is compliant with applicable employment and data protection law.

3. IPR Ownership

One of the biggest drivers for implementing an ESN may be to provide a platform to encourage users to collaborate and generate products, services, and ideas. Yet, this may raise questions of who is entitled to claim intellectual property rights ("IPR") in the content that's created.

In the UK (as in most countries), if the content is generated by employees, IPR will automatically vest in the employer. However, the position is less clear-cut when material is created as a result of collaboration with contractors or third parties. In such circumstances, organisations should consider in advance what is likely to be created and who should own the IPR in such content. In terms of contractors, the relevant contractor or consultancy agreement should ensure that all materials created during the course of the engagement are owned by the company. In terms of third party users, the parties should agree in writing up-front who will own the IPR in any content that is created.

4. IPR Infringement

In addition to the creation of IPR, there is also a risk that employees may infringe IPR via an ESN, for example, by sharing third party materials without consent or in breach of licensing arrangements. Having a clear policy and

training in terms of the use of third party material is essential. Because an ESN is ostensibly an internal network, individuals may not appreciate that sharing third party content via an ESN is very likely to be considered publication under applicable IPR laws and may breach license restrictions (*e.g.*, as to specific group company, number of users, geographical location, etc.)

5. Privacy & Security

An ESN will inevitably involve a large amount of data and a significant proportion of that data may be considered personal data. Organisations will need to identify upfront the nature of personal data likely to be collected, the purposes for which the data will be used, where the data is to be used and by whom, and the appropriate access and security measures that need to be put in place to protect the data. Organisations will then need to ensure that they are compliant with all relevant data protection obligations in terms of such processing.

In particular, where organisations and the ESN operate on an international basis, meaning that personal data of users based within the EEA may be accessed by users outside the EEA (whether employees or third parties), the organisation will need to ensure that appropriate protections are in place to assure that such cross-border transfers are compliant with applicable data protection law.

As discussed above, many ESNs operate as cloud-based solutions, so organisations will also need to make sure that they are comfortable with the potential risks to privacy and security risk posed by a cloud-based solution. If an organisation has a very low risk-appetite (*e.g.*, it operates in a highly regulated sector), it may decide that a cloud-based solution is not appropriate.

CONCLUSION

If you are using a third party ESN, you will also need to put in place an appropriate contract with the provider. Contracts for cloud computing services are generally implemented on the provider's terms and, as we discussed previously in our alert on negotiating cloud contracts, where an ESN is a cloud-based solution, the extent to which a provider's standard terms can be negotiated may be limited. Accordingly, an organisation may decide to focus on certain key issues such as confidentiality, data ownership, privacy, and security.

ESNs provide a "water-cooler" for the digital age and are helping evolve the way organisations communicate. However, organisations must ensure that they put the necessary policies and procedures in place to ensure that it's always good to talk.

Contact:

Susan McLean
+44 20 7920 4045
smclean@mofo.com

Mercedes Samavi
+44 20 7920 4170
msamavi@mofo.com

About Morrison & Foerster:

Client Alert

We are Morrison & Foerster—a global firm of exceptional credentials. Our clients include some of the largest financial institutions, investment banks, Fortune 100, technology and life science companies. We've been included on *The American Lawyer*'s A-List for 11 straight years, and *Fortune* named us one of the "100 Best Companies to Work For." Our lawyers are committed to achieving innovative and business-minded results for our clients, while preserving the differences that make us stronger. This is MoFo. Visit us at www.mofo.com.

Because of the generality of this update, the information provided herein may not be applicable in all situations and should not be acted upon without specific legal advice based on particular situations. Prior results do not guarantee a similar outcome.