proofpoint

November 29, 2010

Proofpoint Predicts Top 10 Privacy Issues for 2011

Social media and location-based technologies top the list for concern

Sunnyvale, Calif. – November 29, 2010 – The prevalence of mobile devices with personally identifiable location-based information and the increasing use of social media are top concerns for 2011, say experts from Proofpoint, Inc., the leading provider of SaaS email security, email archiving and data loss prevention solutions. With more personal information available on the Internet, in everyday consumer applications and stored in corporate databases, risks to consumers and companies will only grow in the next year. In addition, increasing regulations and new laws will force many organizations in 2011 to review their handling of private information and implement new programs to minimize their risks. To deal with these increasing threats and obligations, Proofpoint expects more organizations to create stronger privacy policies and turn to encryption, web filtering and secure managed file transfer.

Proofpoint predicts the following trends will dominate privacy discussions in 2011:

1. The privacy and confidentiality of location-based information will become a major concern for both consumers and corporations. With the rise in mobile GPS information, companies will have to protect both personally identifiable information (PII) of employees, customers and partners, and also create new policies for handling location-based information. Not only will real-time information about location be a vulnerability, but companies will have access to information about where people (or their devices) spend much of their time.

2. At least one major social media site will experience a major breach. According to Neilsen, nearly a quarter (22.7%) of all online time is spent social networking. With more people on social networks and more personal information available via those networks, the potential for exposure of that data is likely.

3. Stricter regulations will be passed worldwide. Privacy regulations in the healthcare, financial services and critical infrastructure industries like energy and telecommunications will likely see new regulations dictating what needs to be protected and what to do when data loss occurs.

4. Expect a national data breach notification law. Notification laws like California's SB 1386 exist in 46 of 50 states today. A federal law is imminent.

5. Blended threats will increase. While email is still the number one threat vector for personal information loss, threats from newer communications channels is increasing, especially in the form of blended threats where the target is first attacked through email, then directed to Web or social media.

6. At least one company will be prosecuted under the broad-reaching Massachusetts Privacy Law (201 CMR 17.00). In March of this year, the Massachusetts Privacy Law went into effect, mandating that any company that "owns or licenses" personal information—whether stored in electronic or paper form—about Massachusetts residents must comply with its privacy requirements, including notification of breaches and encryption of stored or transmitted personal data. Although the state has yet to enforce the law, 2011 will likely be the year that companies begin seeing penalties. In addition, we may see more laws of this type passed in 2011. Nevada also has a similar law.

To deal with these threats, the following additional trends will emerge among businesses:

7. Companies will move away from outright bans on social networks, IM or web mail to allowing those services, but applying stricter corporate policies on these new services as well as investing in secure web gateways to monitor use. New innovations such as Facebook mail give enterprises yet another good reason to put better policy and technology controls around the corporate email system.

8. More companies will create policy around acceptable use. Email leaks such as the recent Google corporate memo exposure are heightening awareness in companies that policies need to be created about what content is considered sensitive and enforce them both through technology and through training.

9. More companies will encrypt more data. Three factors are converging to make 2011 the year of encryption adoption. (1) More regulations today require encryption. (2) It's become a best practice in many industries. (3) It's easier to implement

and less confusing for users. With processing power increasing and companies like Proofpoint innovating, encryption has become faster and easier to implement and use.

10. More interest in secure managed file transfer. Driven by privacy considerations and security flaws in FTP, more companies will be implementing reliable ways to send files securely. With data breach notification laws in place in nearly every state, companies cannot risk losing data through FTP security issues.

To learn more about protecting private data, visit www.proofpoint.com.

About Proofpoint, Inc.
Proofpoint focuses on the art and science of cloud-based email security, eDiscovery and compliance solutions. Organizations around the world depend on Proofpoint's expertise, patented technologies and on-demand delivery system to protect against spam and viruses, safeguard privacy, encrypt sensitive information, and archive messages for easier management and discovery. Proofpoint's enterprise email solutions mitigate the challenges and amplify the benefits of enterprise messaging. Learn more at www.proofpoint.com.

# # #