United States District Court, Middle District of Pennsylvania

Social Network Computer Policy (November, 2009)

The birth and advance of "Web 2.0" technologies and applications in recent years has the potential to revolutionize how individuals, corporations, government agencies, and non-profit organizations interact and communicate with one another. Web 2.0 refers to the second generation of web design and software development, which places heavy emphasis on communication, collaboration, and sharing among internet users. Unlike the first generation of internet (Web 1.0), this change is grounded less in major technical transformations. Instead, this change is centered, chiefly, on the ways individuals use the Internet. Before Web 2.0, most Internet users were mainly consumers of information; now, these new technologies and applications allow users to be both producers and consumers of information and shift easily between those roles.

Many of these Web 2.0 applications, often called "social media," are central parts of many people's daily computer usage. Users, whether they be institutions or individuals, connect and communicate through social networking internet sites; collaborate on, refine, and disseminate knowledge through wikis; share their perspective through blogs and microblogs; upload still and video images through videosharing and photosharing sites; broadcast via podcasts and vodcasts; and stay connected via RSS feeds beamed to e-mail inboxes or displayed on smartphones.

As Web 2.0 has made communication instantaneous and allowed for greater collaboration and information sharing, there has been some downside. Many users adopting Web 2.0 seem less concerned, or at least mindful, of privacy and confidentiality as they navigate social media sites such as Facebook. Recent news stories illustrate the privacy and confidentiality concerns generated by the expansion of social media internet usage: employment opportunities lost because of Facebook profiles; scandal precipitated by YouTube or Flickr postings, and judicial proceedings compromised by jurors' Twitter postings.

The challenges and risks of this social media environment, though, are particularly acute for government employees that work in positions where discretion and confidentiality are imperative. Court employees work in such an environment. Court personnel are expected to keep sensitive information confidential, exercise discretion to avoid embarrassment to the Court, and take precautions to avoid unnecessary security risks for court personnel, especially the judges they serve.

The Court has set down a series of broad guidelines for employees to consider as they navigate these new, and ever changing, technologies and applications.

1. **Think before you post**. Internet postings – whether they be text, photos, videos, or audio – remain accessible long after they are forgotten by the user. Beyond that, remember that nothing is "private" on the Internet despite people's best efforts to keep things private. Do not post anything on the Internet that you would not want to read on the front page of the local or national newspaper.

2. **Speak for yourself, not your institution**. On social networking sites, many individuals list their occupations and/or places of employment. Considering the sensitive nature of the work that we

do, Court employees should carefully evaluate whether the listing of their place of employment on a social networking website poses a security risk.

Also, remember that you are a representative of the Court and should conduct yourself in a way to avoid bringing embarrassment upon yourself and the Court. In the age of Facebook, YouTube and Twitter, many often do not think through the implications of what they post. Users often believe that their postings are private because of a social networking website's privacy features or that their comments are untraceable because they were made under a screen name, but this information may not be private and could cause damage to your reputation and the Court's if it becomes public. As such, Court employees should abide by a simple rule: if you are not speaking to someone directly or over a secure land line, you must assume that anything you say or write is available for public consumption.

3. **Keep secrets secret**. Make sure to abide by all of the court's confidentiality and disclosure provisions. Court employees handle confidential and sensitive information and the restrictions that employees normally observe in the performance of their day-to-day duties should also apply to their use of social media. Just as court employees are prohibited from disclosing sensitive, non-public information to the media and general public in person or over the phone, the same applies to social media. Furthermore, Court employees should refrain from discussing any of the Court's internal processes and procedures, whether they are of a non-confidential or confidential nature.

4. **Remember the Guide**. Any public postings are governed by the Judiciary's Guide to Policies and Procedures. As Judiciary employees, we are expected to avoid impropriety and conduct ourselves in a manner that does not detract from the dignity and independence of the judicial system. As such, Judiciary employees are restricted from engaging in partisan political activity and fund raising activities that could compromise judicial independence. Please keep these policies and procedures in mind as you participate on social media sites.

5. **Observe security protocol**. Court employees must also take care to avoid doing things that would compromise the security of the courthouse and personnel. To maintain security, do not post pictures of the courthouse, inside or outside; do not post pictures of court events and do not post pictures of the Court's judicial officers. Also, be careful when disclosing your place of employment: social media sites are notoriously unsecure environments and knowledge of your place of employment could place employees in situations where pressure could be applied on them to corrupt the integrity of the judicial process.

Our Court reserves the right to monitor its employees' use of Social Media by monitoring its employees' Internet activities as set forth in our Court's Acceptable Use Policy. Our Court further reserves the right to visit and monitor Social Media sites to ensure that employees are not violating our Court's Social Media Policy via Court or any other computers, including employees' own personal computers.