Encyclopedia of Information Systems and Technology

Phillip A. Laplante, Vladimir Stantchev, Jeff Voas, Anne-Marie Smith, Qiuming Zhu, Morris Chang, Irena Bojanova, David Alan Grier, Jia Zhang, Thomas Costello, San Murugesan, Jim Goldman, Joanna DeFranco

Social Networking: Legal, Privacy, and Security Issues

Publication details
Jessica Keyes
Published online on: 29 Dec 2015

How to cite: Jessica Keyes. 29 Dec 2015, Social Networking: Legal, Privacy, and Security Issues from: Encyclopedia of Information Systems and Technology CRC Press
Accessed on: 18 Aug 2023

PLEASE SCROLL DOWN FOR DOCUMENT

Full terms and conditions of use: https://www.routledgehandbooks.com/legal-notices/terms

This Document PDF may be used for research, teaching and private study purposes. Any substantial or systematic reproductions, re-distribution, re-selling, loan or sub-licensing, systematic supply or distribution in any form to anyone is expressly forbidden.

The publisher does not give any warranty express or implied or make any representation that the contents will be complete or accurate or up to date. The publisher shall not be liable for an loss, actions, claims, proceedings, demand or costs or damages whatsoever or howsoever caused arising directly or indirectly in connection with or arising out of the use of this material.
Social Networking: Legal, Privacy, and Security Issues

Jessica Keyes

Abstract
This entry presents legal barriers easily overlooked in social networking. Privacy issues are discussed, as well as potential breaches of security.

Do these facts concern you?

- When you buy a Microsoft Kinect, you bring into your home or office a telescreen that can recognize who’s in the room and interpret body language.
- A joint effort by a British university and a Canadian security company will bring to a theater near you the ability to monitor facial expressions.
- Cisco commissioned a survey of 2600 workers and information technology (IT) professionals in 13 countries. Twenty percent of the IT leaders said that their relationships with their employees were dysfunctional—demonstrating a disconnect among IT, employees, and policies.
- A recent survey of 1100 mobile workers found that 22% had breached their employers’ strict smartphone policies when using nonmanaged personal smartphones to access corporate information.
- One in eight malware attacks is accomplished via a Universal Serial Bus (USB) device, according to Avast Software, a security firm.
- A virus may be transmitted by any connected device, for example, MP3 players, cameras, fax machines, and even digital picture frames. In 2008, the Best Buy chain found a virus in the Insignia picture frames it sold.
- Companies outsourcing data storage (to a cloud) are responsible for any data breached. Make sure your cloud or data service provider is investigated carefully.
- Cybercriminals are getting smarter. They invented poisoned search results, rogue anti-viruses (AVs), social networking malware, malicious advertisements, and even built-in instant messaging clients that notify criminals when their “marks” have logged onto their online bank accounts.

Social networking raises some issues concerning content use, infringement, defamation, attribution, tort liability, privacy, and security. While most of these issues relate to public social networking sites such as Facebook and LinkedIn, most are also relevant to internal social software engineering, particularly if public platforms are integrated into the toolsets.

WEBSITE LEGAL ISSUES

Defamation and other torts—Wikis, blogs, workspaces, and other IT facilities provide ample opportunities for defamation (harming the reputation of another by making a false statement to a third person). These resources should be monitored for possible defamation and other tort liabilities. Examples of damages arising from torts include intentional infliction of emotional distress, interference with advantageous economic relations, fraud, and misrepresentation.

Trademarks—Trademark or service mark notices should be notably displayed wherever required. If a mark has been registered with the U.S. Patent and Trademark Office (http://www.uspto.gov/), the “registered” (®) symbol should be displayed; otherwise, the trademark (TM) or service mark (SM) symbol should be displayed. Organizations should be vigilant in protecting their trademarks and service marks, and equally vigilant in preventing infringements on the marks of others. Content that resides on an organization’s servers should be audited to ensure no trademark infringement is taking place.

Copyrights—Copyright is a form of protection provided to the authors of “original works of authorship” including literary, dramatic, musical, artistic, and other types of intellectual works such as software, both published and unpublished. The 1976 Copyright Act
generally gives the owner of a copyright the exclusive right to reproduce the copyrighted work, prepare derivative works, distribute copies or audio recordings of the copyrighted work, perform the copyrighted work publicly, and display the copyrighted work publicly. A copyright protects the form of expression rather than the subject of the writing. For example, a description of a machine could be copyrighted, but doing so would only prevent others from copying the description; it would not prevent others from writing their own descriptions or from making and using the machine.

It is important for organizations to audit data residing in their social networks to make sure that any content, data, and information is not violating copyrights of other individuals or organizations. One example is dynamically accessing Google and downloading research results to a social network. Because Google’s content is copyrighted to Google, you would need to take care not to violate any copyrights. Using third-party content without permission can result in both criminal and civil liability, including treble damages and attorney fees under the U.S. Copyright Act. Essentially, the best tactic is to periodically review network content to screen for possible copyright violations.

Computer Fraud and Abuse Act (CFAA)—Most organizations provide their employees with PCs capable of wireless Internet access. Many companies and home users have installed wireless Internet connectivity. It is not usual for people to seek out unsecured “hot spots,” as these wireless connections are known. Several computer equipment manufacturers have developed inexpensive, small hot-spot locaters for this purpose. The CFAAmakes it punishable for whoever intentionally accesses a computer without authorization. Organizations must develop very clear policies warning employees against using corporate-supplied PCs in this manner.

Corporate content—Not long ago, a Congressman made a secret trip to Iraq. Upon arrival, he tweeted a message that he had just landed. His trip was no longer a secret. While we have not focused on the use of Twitter as a social software engineering tool, we expect Twitter or its corporate equivalent, Yammer to be used. Because these systems enable almost instantaneous communication with an entire network of people within and outside an organization, users must be very careful about exactly what they communicate.

DEVELOPING YOUR ePOLICY

It is important that the organization develop an ePolicy that addresses how employees use email, Internet access, and all social networking activities. The policy should be comprehensive, appear in the employee handbook, and be reviewed with all new employees. It is also a good idea to refresh the memories of all employees annually by sending an e-mail, instructing them to review the ePolicy. The policy should be stored on the corporate intranet, and one staff member should be assigned as the main point of contact for the ePolicy, if questions or problems arise. Some points to address in an ePolicy include

- Whether employees may use the Internet for personal use.
- Whether external social networking services such as Facebook, LinkedIn, and Yammer may be used.
- Notice that e-mail is monitored (if it is not, it should be). Let employees know that the e-mail and social networking systems they use are owned by the organization, and they can expect that management or designated staff may access e-mail, workspaces, blogs, wikis, etc.
- Descriptions of the types of content that can be maintained within internal or external social networking site, e.g., copyrighted materials.
- Netiquette policies for using e-mail and social networking websites.
- Details of corporate discrimination and sexual harassment policies, particularly as they relate to online environments.
- The expectation that individual employees will respect the privacy of the individuals whose information they may access, and use all available security methods to preserve the integrity and privacy of information within their control.
- A directive that specifies that employees are not to engage in any activity that alters or damages data, software, or other technological-related resources belonging to the organization or to someone else; compromise another individual’s ability to use technological-related resources; or intentionally disrupt or damage corporate technology resources.
- A stipulation that individuals who observe potential abuse are expected to report it for appropriate resolution.

SECURITY ISSUES

In 2008, Cisco commissioned a study on security in the workplace. The study findings will probably not surprise you:

- One of five employees altered security settings on work devices to bypass IT policy to access unauthorized web sites. More than half said they simply wanted to access the sites; a third indicated that the sites they accessed “were no one’s business.” Seven
out of ten IT professionals said employee access of unauthorized applications and websites ultimately resulted in as many as half of their companies’ data loss incidents. This belief was most common in the United States (74%) and India (79%).

- Two of five IT pros dealt with employees accessing unauthorized parts of a network or facility. Of those who reported this issue, two-thirds encountered multiple incidents in the past year, and 14% encountered it monthly.
- One in four employees admitted verbally sharing sensitive information with nonemployees such as friends, family, and even strangers. When asked why, the most common answers included, “I needed to bounce an idea off someone,” “I needed to vent,” and “I didn’t see anything wrong with it.”
- Almost half of the employees surveyed share work devices with others, including nonemployees without supervision.
- Almost two out of three employees admitted using work computers daily for personal use. Activities included music downloads, shopping, banking, blogging, and participating in chat groups. Half of the employees used personal e-mail to reach customers and colleagues; only 40% said such use was authorized by IT.
- At least one in three employees left computers logged on and unlocked when they left their desks. They also tended to leave laptops on their desks overnight, sometimes without logging off, creating potential for theft and allowing unauthorized access to corporate and personal data.
- One in five employees stored system log-ins and passwords in their computers or wrote the information and left it on their desks, in unlocked cabinets, or pasted on the front of their computers.
- Almost one in four employees carried corporate data on portable storage devices outside the office.
- More than one in five employees allowed nonemployees to roam around offices unsupervised. The study average was 13%; 18% allowed unknown individuals to “tailgate” behind employees into corporate facilities.

As you can see, information systems (ISs) are vulnerable to many threats that can inflict various types of damage, resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire systems centers. Problems can arise from inside the company (employees) to the more common scenario such as outsiders intent on harm. All manner of hardware and software is at risk, including mobile devices. In 2010, we all awoke to the news that iPad users’ e-mail addresses and device user identifications (IDs) were exposed. In 2009, security experts identified 30 security flaws in the software and operating systems of smartphones. Also in 2010, two European university researchers extracted an entire database of text messages (including deleted messages) from an iPhone using a corrupt website they controlled.

Losses from these exploits can stem, for example, from the fraudulent actions of supposedly trusted employees, outside hackers, or careless data entry. An organization should develop an ISs security program to implement and maintain the most cost-effective safeguards to protect against deliberate or inadvertent acts, including

1. Unauthorized disclosure of sensitive information or manipulation of data
2. Denial of service or decrease in reliability of critical IS assets
3. Unauthorized use of systems resources
4. Theft or destruction of system assets

An extremely detailed checklist of best practices for security has been compiled by the U.S. Department of Defense. It covers access control, confidentiality, integrity, availability, non-repudiation, protection, detection, reaction to incidents, configuration management, vulnerability management, personnel security, physical security, and security awareness and training. All of these topics should be reviewed before initiating any social software engineering program from setting the parameters for its use. The checklist should also be used on a periodic basis to ensure the security of the social software engineering platform on an ongoing basis. The organization should develop an IS security plan to meet the following goals:

1. Achieve data integrity levels consistent with the sensitivity of the information processed.
2. Achieve systems reliability levels consistent with the sensitivity of the information processed.
3. Comply with applicable state and federal regulations.
4. Implement and maintain continuity of operations plans consistent with the criticality of user information processing requirements.
5. Implement and follow procedures to report and act on IS security incidents.

Organizations should conduct periodic security reviews to ensure that

1. Sufficient controls and security measures are in place to compensate for any identified risks associated with the program/system or its environment.
2. The program/system operates cost effectively and complies with applicable laws and regulations.
3. The information in the program/system is properly managed.
4. The program/system complies with management, financial, IT, accounting, budget, and other appropriate standards.

Two types of security assessments of computer facilities must be conducted periodically: risk assessments and security reviews. A risk assessment is a formal, systematic approach to assessing the vulnerability of computer assets, identifying threats, quantifying potential losses from threat realization, and developing countermeasures to eliminate or reduce threats and potential losses. Risk assessments should be conducted whenever significant modifications are made to the system.

The three major IT security components are management controls, operational controls, and technical controls. The management controls address matters deemed managerial. The technical controls are security measures that should be implemented on systems that transmit, process, and store information. The operational controls address security measures implemented by employees that directly support the technical controls and processing environment.

Management controls are necessary to manage a security program and its associated risks. They are non-technical techniques, driven by policy and process, and are intended to meet IT protection requirements. Program security policies and system-specific policies are developed to protect sensitive information, transmitted, stored, and processed within system components. Program security policies are broad and are developed to establish a security program and enforce security at the program management level. System-specific security policies are detailed and developed to enforce security at the system level. The information, applications, systems, networks, and resources must be protected from loss, misuse, and unauthorized modification, access, and compromise. All organizations that process, store, or transmit information must develop, implement, and maintain IT security programs, to ensure protection of their information. The program security policy establishes the program, assigns the appropriate personnel, and outlines the duties and responsibilities of all individuals in the program.

Operational controls focus on controls implemented and executed to improve the security of a particular system. Media controls address the storage, retrieval, and disposal of sensitive materials that should be protected from unauthorized disclosure, modification, and destruction. Media protection is composed of two security requirements: computer output controls and electronic media controls. Computer output controls apply to all printout copies of sensitive information, and specify that all printout copies of sensitive information should be clearly marked. Electronic media controls should encompass all the controls of printout materials; however, procedures must be established to ensure that data cannot be accessed without authorization and authentication from electronic media that contain sensitive information.

All personnel with responsibilities for the management, maintenance, operations, or use of system resources and access to sensitive information should have the appropriate management approvals. Organizations should institute personnel security procedures to specify responsibilities of the security personnel and users involved in the management, use, and operation of systems. The IT staff must be alert and trained in offensive and defensive methods to protect the organization’s information assets. Adequate staffing and key position back-up are essential in maintaining a secure environment. Personnel security also includes establishing and maintaining procedures for enforcing personnel controls, including

- Determining appropriate access levels (logically and physically)
- Ensuring separation of duties (logically and physically) to prevent compromise of system data and attempts to thwart technical controls
- Conducting security training and providing awareness tools for all staff
- Issuing and revoking IDs and passwords

Technical controls focus on security controls that the computer system executes, and they rely on the proper configuration and functionality of the system. The implementation of technical controls always requires significant operational considerations. Technical controls should be consistent with the management of security within the organization. When updating a security plan, the organization should refer to the security issues and questions, as shown, in Table1 to ensure its plan remains current.

WEB SERVER SECURITY

Securing the operating system that runs the web server is the initial step in providing security for the server. The web server software differs only in functionality from other applications that reside on computers. However, because the web server may provide public access to the system along with organization-wide access, it should be configured securely to prevent it and the host computer from being compromised by intruders.

One precaution to take when configuring a web server is to never run the Web service as a root or administrative user (super user). Web services or applications should never be located at the root of a directory structure. They should be in a component-specific subdirectory to provide
optimum access management. The Web service should be run with the permissions of a normal user to prevent the escalation of privilege if the web server were compromised. Also, the file system of the web server (directories and files) should be configured to prevent write access for any users other than authorized employees who require such access. Other precautions and secure configuration issues to consider when configuring a public web server are:

- The web server should be on a separate local area network separated from other production systems by a firewall configuration or demilitarized zone (DMZ).
- The web server should never have a trust relationship with any other server that is not also an Internet-facing server or server on the same local network.
- The web server should be treated as an untrusted host.
- The web server should be dedicated to providing Web services only.
- Compilers should not be installed on the web server.
- All services not required by the web server should be disabled.
- The web server should utilize the latest vendor software, including hot fixes and patches.

A Web browser is usually a commercial client application used to display information requested from a web server. It should be a standard browser approved for use within the system environment. Because of the security holes in scripting languages not required for official systems operation be disabled within the browser.

Network security addresses requirements for protecting sensitive data from unauthorized disclosure, modification, and deletion. Requirements include protecting critical network services and resources from unauthorized use and security-relevant denial-of-service conditions.

Firewalls provide greater security by enforcing access control rules before connections are made. These systems can be configured to control access to or from the protected networks, and are most often used to shield access from the Internet. A firewall can be a router, a personal computer, or a host appliance that provides additional access control to the site. The following firewall requirements should be implemented:

- Firewalls that are accessible from the Internet are configured to detect intrusion attempts and issue an alert when an attack or attempt to bypass system security occurs.
- Firewalls are configured to maintain audit records of all security-relevant events. The audit logs are archived and maintained in accordance with applicable records retention requirements and security directives.
- Firewall software is kept current with the installation of all security-related updates, fixes, and modifications, as soon as they are tested and approved.
- Firewalls should be configured under the “default deny” concept. This means that activation of a service or port must be approved for specific use. By
default, the use of any service or communications port without specific approval is denied.
- Only the minimum set of firewall services necessary for business operations is enabled, and only with the approval of IT management.
- All unused firewall ports and services are disabled.
- All publicly accessible servers are located in the firewall, DMZ, or an area specifically configured to isolate these servers from the rest of the infrastructure.
- Firewalls filter incoming packets on the basis of Internet addresses to ensure that any packets with internal source addresses received from external connections are rejected.
- Firewalls are located in controlled access areas.

Routers and switches provide communication services that are essential to the correct and secure transmission of data on local and wide area networks. The compromise of a router or switch may result in denial of service to the network and exposure of sensitive data, which can lead to attacks against other networks from a single location. The following best-practice solutions should be applied to all routers and switches throughout an application environment:

- Access to routers and switches is password-protected in accordance with policy guidance.
- Only the minimum set of router and switch services necessary for business operations is enabled and only with the approval of IT management.
- All unused switch and router ports are disabled.
- Routers and switches are configured to maintain audit records of all security-relevant events.
- Router and switch software is kept current by installing all security-related updates, fixes, and modifications, as soon as they are tested and approved for installation.
- Any dial-up connections via routers must be performed by a method approved by IT management.

All systems should use AV utilities or programs to detect and remove viruses and other malicious codes. The AV software must be kept current with the latest available virus signature files installed. AV programs should be installed on workstations to detect and remove viruses in incoming and outgoing e-mail messages and attachments, and also actively scan downloaded files from the Internet. Workstation and server disk drives should be routinely scanned for viruses. The specific restrictions outlined below should be implemented to reduce the threat of viruses on systems:

1. Traffic destined to inappropriate websites should not be allowed.
2. Only authorized software should be introduced on systems.
3. All media should be scanned for viruses before introduction to the system. This includes software and data from other activities and programs downloaded from the Internet.
4. Original software should not be issued to users but should be copied for use in copyright agreements. At least one copy of the original software should be stored according to configuration management controls.

Table 2 outlines the topics of a systems security plan. During development of a security plan, the following questions should be asked and answered:

1. Does the plan address the logical and physical security of the system?
2. Does the logical security include password protection, data encryption (if applicable), and access profiles, to preclude access to data by unauthorized personnel?
3. Does the logical security allow supervisory intervention if needed (determined case by case)?
4. Are negotiable documents or authorizations stored securely?
5. Does the physical security address both equipment security and building security?
6. Does the physical security address safety and environment issues?
7. Does the security plan address data and application back-up procedures?
8. Does the security plan include disaster preparedness and recovery procedures? (They may appear in a separate plan.)
9. If a department or organization-wide security plan exists is the point where the system security plan stops and the organization plan takes over (and vice versa) delineated clearly?
10. Does the logical security include separation of duties among functions to prevent potential fraud situations?

**PROTECTING MOBILE DEVICES**

Many people ignore security policies pertaining to their smartphones. They seem not to realize how they may be exposing themselves, their companies, and their companies’ stakeholders to harm. While mobile devices cannot be totally secured, certain measures afford some measure of security:

1. Do not use hotel wireless networks to access sensitive information.
2. Hotel wired networks are often open to eavesdropping. All packets for a set of rooms, a floor or
several floors, or even an entire hotel can be seen by all other systems on the network. Unprotected packets are prime targets for capture, analysis, and data extraction. A company should invest in wireless broadband equipment for employees who must travel and bring their work with them.

3. Encrypt all data on a device in case it is stolen or lost—a common occurrence. Better yet, store information on the server or in the cloud, not on the device.

4. Configure devices to block external snooping. Firewalls are required and are available for many handheld devices.

5. Backup critical information. This sounds obvious, but employees on the road may neglect to do this. If the organization does not have a mobile-accessible back-up server, use a cloud service such as Microsoft Skydrive (skydrive.login.com).

6. Do not start a laptop with a USB device attached. This can result in direct loading of malware ahead of antivirus software.

7. Secure all wireless access points. Strong, mixed passwords should be used and changed frequently.

Table 2 Systems security plan

<table>
<thead>
<tr>
<th>Topic Outline</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Scope—Describe site, giving location, configuration, operations, processing supported, and identify IT units and applications covered by plan</td>
</tr>
<tr>
<td>2. Definitions—Explain terms that may not be familiar to all readers</td>
</tr>
<tr>
<td>3. Overall security assessment—Discuss policies and practices, addressing assignment of security responsibilities, personnel security clearance policies, audit reports, and training; also assess current activities and plans for next year</td>
</tr>
<tr>
<td>4. Site plan and equipment schematic diagrams</td>
</tr>
<tr>
<td>5. Obtain the following information for each sensitive application system: date of last system evaluation, date of last system certification or recertification, date of next evaluation or recertification</td>
</tr>
<tr>
<td>6. Summary of risk analysis reports</td>
</tr>
<tr>
<td>7. Continuity plan (s)</td>
</tr>
<tr>
<td>8. Summary of security reviews for all processing platforms in use</td>
</tr>
<tr>
<td>9. Training needs with action schedules</td>
</tr>
<tr>
<td>10. Other supporting documents (terminal security rules, local security procedures, user handbooks, etc.)</td>
</tr>
</tbody>
</table>

Policies and Procedures

| 1. Physical security of resources |
| 2. Equipment security to protect equipment from theft and unauthorized use |
| 3. Software and data security |
| 4. Telecommunications security |
| 5. Personnel security |
| 6. Continuity plans to meet critical processing needs during short- or long-term interruption of service |
| 7. Emergency preparedness |
| 8. Designation of IT security officer or manager |