BRYAN CAVE
A Broader Perspective
Bulletin

Data Privacy & Security Team

To: Our Clients and Friends June 19, 2012

What do video game, music, and free online telephone networks have in common? If your employees use them they can lead to a FTC data security investigation

Although the days of Napster and Gnutella may be over, the technology upon which those applications were based – peer-to-peer networks or "P2P" – is alive and well in modern day programs that share video games and music such as BearShare, LimeWire, KaZaa, eMule, Vuze, uTorrent and BitTorrent. As two recent Federal Trade Commission ("FTC") enforcement actions illustrate, companies that permit employees to use P2P applications – either knowingly or unknowingly – may face government investigations and possible liability.

The data security risk of P2P applications

For several years the FTC has warned businesses that P2P applications can lead to a data security breach if the application is installed on a computer that contains sensitive information, or is itself part of a network that contains sensitive information. Specifically, P2P programs can contribute to a breach if:

- A user inadvertently allows the P2P program to share drives, files, or folders that contain sensitive information,
- A virus or malware changes the drives or folders designated for P2P sharing, or
- The P2P program has security flaws that permit hackers to attack the computer, or other networks to which the computer is connected.

P2P Related Data Breaches

To-date the FTC has identified almost one hundred data breaches which it suspects were caused by an employee using a P2P application. In addition to sending a series of warning letters to companies, earlier this week the FTC announced law enforcement actions against two companies – EPN, Inc. and

Franklin Toyota/Scion - relating to breaches allegedly caused by their employees' use of P2P applications.

The complaints allege that employees within both companies used P2P applications on company owned computers. Although neither complaint reveals how many employees were using such programs, in one case the FTC alleged that a P2P application had been used by an executive level employee – the company's Chief Operating Officer. According to the complaints, breaches involving the use of the P2P applications led to information relating to 98,800 consumers being made available on P2P networks. In addition, the FTC specifically cited both companies for failing to have an incident response plan in place to limit the extent of the breaches once they were identified.

Both companies have agreed to settle the FTC's investigation. As part of the settlement they have agreed to have their security programs reviewed by a third party for the next 20 years.

Limiting risks associated with P2P applications

Based upon the FTC's enforcement actions, companies should consider the feasibility of revising their information security program to:

1. Prohibit employees at all levels – including managers and executives – from using P2P applications,

2. Block employees from accessing sites used to download P2P file sharing programs,

3. Block employees from installing applications on workstations without administrator consent,

4. Implement technology to scan computer terminals and networks to identify unauthorized P2P file sharing applications, and

5. Monitor traffic using intrusion detection systems ("IDS"), intrusion prevention systems ("IPS") or firewalls to detect P2P traffic.

For further information on this topic, please contact David Zetoony at 202-508-6030, Jason Haislmaier at 303-417-8503 or any member of the Bryan Cave Data Privacy & Security Team.

In addition, if you experience a data security breach and are not able to contact a member of the Team directly, you can call Bryan Cave's Data Breach Hotline 24 hours a day, 7 days a week at +1 202 508 6136 (international) or +1 888 474 9743 (toll free – US only).

Bryan Cave's Briefings are available online at www.bryancave.com/bulletins.