Testimony before the House Committee on Oversight and Government Reform

Robert Boback, CEO, Tiversa, Inc.

July 29, 2009

Good morning Chairman Towns, Ranking Member Issa and Distinguished Members of the Committee.

My name is Robert Boback and I am the Chief Executive Officer of Tiversa, a Pennsylvania-based company that provides security and intelligence services to help protect organizations from the disclosure and illicit use of sensitive, confidential, and personal information on peer-to-peer file sharing, or "P2P", networks.

P2P file-sharing continues to be a major security risk and privacy issue. Today, I will provide a brief background on P2P networks, highlight the risks of inadvertent file sharing, provide examples of P2P file disclosures and the impact on consumers, businesses, government, the military and national security, and share our observations and recommendations.

Background: Peer-to-Peer Networks

The Internet is comprised essentially of four components: World Wide Web, Instant Messenger (IM), Email, and Peer-to-Peer networks. By many accounts, the largest of these by measure of consumption of overall bandwidth is Peer-to-Peer or P2P. This distinction is necessary to understand the security implications that we are presented with today as a result of both the enormity of the networks as well as the different security challenges that are presented by the networks.

P2P networks have been in existence for several years starting most notoriously with the introduction of Napster in the fall of 1999. The P2P networks have provided a gateway for users around the world to share digital content, most notably music, movies and software.

P2P networks are growing and dynamic. Since 2005, P2P networks have grown at the rate of over 20% (CAGR). Today, worldwide P2P networks may have over 20 million users at any point in time. P2P networks are ever-changing as users join and exit constantly. The number of P2P programs or "clients" has grown to over 225, with many having multiple versions in use. Additionally, many of the programs are open source and, accordingly, subject to modification as users see fit. P2P networks are a worldwide phenomenon with users across wide ranges of ages, educational backgrounds and incomes.

The use of P2P has evolved and is used by individuals worldwide for many different purposes including:

1 – Planned file sharing – its intended use.
2 – Searching for information with malicious intent – personal information used in identity theft; corporate information and trade secrets; and even military secrets and intelligence.
3 – Distribution and sharing of illegal information – Child pornography and information that could be used in terror activity.

Inadvertent File Disclosure

P2P networks continue to grow in size and popularity due to the extent of the content that is present and available on the networks, that in many cases, is not available from any other public source. In addition to movie and music files, millions of documents, that were not intended to be shared with others, are also available on these networks. It is this unintentional sharing that we refer to as inadvertent sharing or disclosure.

Inadvertent sharing happens when computer users mistakenly share more files than they had intended. For example, they may want to share only their music files or a large academic report, but instead expose all files on their computer's hard drive allowing other users to have access to their private or sensitive information. This can occur via several scenarios. These scenarios range from user error, access control issues (both authorized and unauthorized), intentional software developer deception, to malicious code dissemination.

"User error" scenario occurs when a user downloads a P2P software program without fully understanding the security ramifications of the selections made during the installation process. This scenario has been decreasing slightly in the past few years as many of the leading P2P clients have highlighted the security risks associated with sharing various types of files containing sensitive information.

"Access control" occurs most commonly when a child downloads P2P software program on his/her parents' computer. This may occur with or without the parents' knowledge or consent, however the sensitive or confidential information stored on that computer may become exposed publicly nonetheless.

“Intentional software developer deception” occurs when the P2P developers knowingly and intentionally scan and index any or all information during the installation process without the consent of the user. This practice was widely used a few years ago in an effort to populate the P2P networks with large amounts of content. The average user has no incentive to share any files with the other users on the network, confidential or not. The P2P developers recognized that this fact could cause a lack of content to be shared which would negatively impact the network itself. In recent years and in response to legislative intervention and awareness, most mainstream developers have discontinued this controversial tactic. However, there are over 225 P2P software programs that Tiversa has identified being used to access these networks. Many of these programs continue to surreptitiously index and share files in this fashion.

“Malicious code dissemination” occurs when identity thieves, hackers, fraudsters, and criminals embed malicious code (“worms”) in a variety of files that appear innocuous. This scenario is extremely troubling as this malicious code can either force a system to reset its preconfigured security measures, despite the security-focused intentions of the P2P developers, or it can install an aggressive P2P program on a user’s computer who may have never intended to install a P2P file sharing program. This scenario can expose even the most technologically advanced consumer or even an individual who has never intended to use P2P to identity theft or fraud. It can also lead to the inadvertent disclosure of sensitive work-related information that can inflict significant economic or brand damage to an organization and/or lead to the identity theft of customers, employees, or others.

The fact that P2P involves downloading of files from individuals that are unknown to the downloader allows the hacker to overcome the hurdle of getting users to download the worm. These criminals intentionally give the malicious code as the same name as highly sought after music, movie, and software downloads to ensure rapid and effective dissemination. Other criminals will use email attachments embedded with aggressive software that mimics P2P programs when installed. These worms will index and share all information on the victim’s computer without any visibility to the victim. This code is very insidious as users cannot detect its presence on their systems. Current anti-virus programs typically do not detect the presence of such malicious software as it appears to the detection software as an intentionally-downloaded standard P2P software program. It is also important to note that firewalls and encryption do not address or protect the user from this type of disclosure.

These scenarios have resulted in millions of highly sensitive files affecting consumers, businesses large and small, the U.S. government, our financial infrastructure, national security, and even our troops being exposed daily to identity thieves, fraudsters, child predators, foreign intelligence organizations and terrorists worldwide.

Despite the tools that P2P network developers are incorporating into their software to avoid the inadvertent file sharing of private and classified information, this significant and growing problem continues to exist. Any changes made to the P2P software, while welcome and helpful, will not fully address the problem. Combine this with the fact that today’s existing safeguards, such as data loss prevention, firewalls, encryption, port-scanning, policies, etc, simply do not effectively mitigate peer-to-peer file-sharing risk.

Warnings regarding inadvertent file sharing through P2P networks have been sounded in the past. The FTC issued warnings on exposing private information via P2P mechanisms. The 2003 Government Network Security Act highlighted the dangers facing government agencies and prescribed a course of action. Prominent security organizations, such as CERT (Computer Emergency Response Team) and the SANS Institute have warned corporations, governments, and consumers to the unintended dangers of inadvertent file sharing via P2P networks.

For example, CERT’s ST05-007-Risks of File Sharing Technology – Exposure of Sensitive or Personal Information clearly states:

> *“By using P2P applications, you may be giving other users access to personal information. Whether it’s because certain directories are accessible or because you provide personal information to what you believe to be a trusted person or organization, unauthorized people may be able to access your financial or medical data, personal documents, sensitive corporate information, or other personal information. Once information has been exposed to unauthorized people, it’s difficult to know how many people have accessed it. The availability of this information may increase your risk of identity theft.”*

In July 2007, the House Committee on Oversight and Government Reform held a hearing on the very issue of the “Inadvertent Sharing via P2P Networks,” during which many of the individuals that testified assured the Committee that this problem was being addressed or being remedied. Despite this recognition, most consumers and security experts at corporations worldwide have very little understanding of the information security risks caused by P2P. Most corporations believe that the current policies and existing security measures will protect their information – they will not.

Today, we will provide the Committee with concrete examples that show the extent of the security problems that exist on the P2P networks and the implications of sharing this type of information. During our testimony, we will provide the Committee with examples that illustrate the types of sensitive information available on P2P networks, provide examples of how identity thieves and others are actively searching for and using the information harvested from these networks, and offer our thoughts on actions to address the problem.

During our testimony today, we will show evidence that despite the numerous warnings and assurances by the developers and government agencies in previous hearings, the problem remains. In fact, we will also demonstrate the unprecedented increase in identity thieves using P2P software programs to harvest consumer information.

It is important to note that Tiversa believes strongly in the useful technology that is P2P. P2P file sharing is one of the most powerful technologies created in recent years, however, as with the World Wide Web, it is not without its inherent risks.

Tiversa and its Technology

Beginning in 2003, Tiversa developed systems that monitor and interact with and within P2P networks to search for sensitive information in an effort to protect the confidential information of our clients. The technology has been designed, developed and implemented in a way that is transparent to the network; in a way that preserves the network's sustainability.

Tiversa centralizes what was previously a decentralized P2P file-sharing network. Tiversa can see and detect all the previously untraceable activity on the P2P network in one place to analyze searches and requests. While an individual user can only see a very small portion of a P2P file sharing network, Tiversa can see the P2P network in its entirety in real time. With this platform, Tiversa has processed as many as 1.6 billion P2P searches per day, more than the number of web searches entered into Google per day. This unique technology has led some industry experts (Information Week) to refer to Tiversa as the "Google of P2P."

Tiversa uses this technology to provide P2P security and intelligence services to businesses, consumers and law enforcement agencies. The following examples demonstrate how inadvertent breaches affect individual consumers, businesses, government, military and national security and are based on our unique perspective on P2P networks.

Examples: Inadvertent Disclosures on P2P

Consumers

Financial Fraud – From analysis of P2P searches, listed below is a small sampling of actual searches issued on P2P networks during a brief research window in March 2009. The term *credit card* was used as the filter criteria for the period.

- *2007 credit card numbers*
- *2008 batch of credit cards*
- *2008 credit card numbers*
- *a&l credit card*
- *aa credit card application*
- *abbey credit cards*
- *abbey national credit card*
- *ad credit card authorization*
- *april credit card information*
- *athens mba credit card payment*
- *atw 4m credit card application*
- *austins credit card info*
- *auth card credit*
- *authorization credit card*
- *authorization for credit card*
- *authorize net credit card*
- *bank and credit card informati*
- *bank credit card*
- *bank credit card information*
- *bank credits cards passwords*
- *bank numbers on credit cards*
- *bank of america credit cards*
- *bank of scotland credit card*
- *bank staffs credit cards only*
- *barnabys credit card personal*
- *bibby chase credit card*

As evidenced by the sampling above, it is clear to see that malicious individuals are issuing searches on P2P networks to gain access to consumer credit cards. Criminals will quickly use the information located to commit fraud using the stolen credit information. This fact was proven during our research with Dartmouth College and published in their subsequent report.

The term "tax return" is also highly sought after on P2P networks. During a live demonstration in January of this year for NBC's Today Show, Tiversa was able to locate and download over 275,000 tax returns from one brief search of the P2P. Many of these individuals have either saved an electronic copy of their tax return that they prepared themselves or have saved an electronic copy of their tax return that an accountant or professional tax office had prepared for them. There are also cases in which accountants and tax offices, themselves, inadvertently disclosed client tax returns.

It is a fact that identity thieves search for tax returns to primarily gain access to Social Security Numbers ("SSN"). According to a report on the black market, SSNs are worth approximately $35 each. This is up from approximately $8-$10 only a few short years ago. One plausible explanation for the rapid increase in black market pricing is that identity thieves are finding better ways to now monetize the stolen SSNs. This is a very important point. Our search data shows that thieves in fact employ a new degree of sophistication in cyber crime.

Identity thieves will also file an individual's tax return before the actual individual files the return. The thief will use a fabricated W-2, which can be printed using a number of programs, and will attempt to steal the phony refund that results from the fabricated return. When the victim then files his or her legitimate tax return, it will automatically be rejected by the IRS as "already filed." Eventually, the IRS will determine that the information, provided by the criminal on the W-2, doesn't match the records that it maintains. At this point, the criminal has most likely cashed the check from the fraud and has moved on to other victims leaving the initial victim to address the problem with the IRS. This is very costly and time consuming for both the victim and the IRS.

Stolen SSNs are also used by illegal aliens to gain employment in the United States. This crime has far reaching implications as well as placing a tremendous tax burden on the victim.

Medical Fraud – Medical information is also being targeted on P2P networks with alarming and increasing regularity. Listed below are some terms issued over the same period regarding medical information.

- *letter for medical bills*
- *letter for medical bills dr*
- *letter for medical bills etmc*
- *letter re medical bills 10th*
- *ltr client medical report*
- *ltr hjh rosimah medical*
- *ltr medical body4life*
- *ltr medical maternity portland*
- *ltr medical misc portland*
- *ltr orange medical head center*
- *ltr to valley medical*
- *lytec medical billing*
- *medical investigation*
- *medical journals password medical .txt*
- *medical abuce records*
- *medical abuse*
- *medical abuse records*
- *medical algoritms*
- *medical authorization*
- *medical authorization form*
- *medical authorization*
- *medical benefits*
- *medical benefits plan chart*
- *medical biliing*
- *medical biling*
- *medical bill*
- *medical biller resume*
- *medical billig software*
- *medical billing*
- *medical billing windows*

Identity thieves and fraudsters use medical information very similarly to financial information, but with much less scrutiny on behalf of law enforcement.

For example, if an identity thief were to download a consumer's medical insurance information, the thief would immediately have access to significant financial resources (in many cases medical insurance policies have limits set at $1 million or above). The criminal would most likely use the insurance card to buy online pharmaceuticals (predominantly Oxycontin, Viagra, or Percoset) which can be quickly sold for cash. This is a very difficult crime to detect as many consumers do not read Explanation of Benefit (EOB) forms sent from the insurance company, prolonging the criminal activity by delaying detection. Even consumers who do read the forms may not readily understand the diagnosis and treatment codes that are indicated on the forms. The victimization of the consumer continues when he or she attempts to appropriately use his or her insurance information for valid medical services only to be turned away or confronted with the suggestion of a potential prescription drug addiction.

User-issued P2P searches attempting to access financial, accounting, and medical information have risen 59.7% since September 2008. For the years of 2006 and 2007, the average annual rise in the search totaled just over 10%.

Child Predation – As if the aforementioned fraudulent activities were not enough to demonstrate the security implications of having personally identifiable information (PII) available to the public on these networks, the crimes can be even more heinous.

Tiversa works with federal, state, and local law enforcement agencies to address the rampant child pornography issues that permeate the P2P file sharing networks. The task is large and process is long however we continue to make progress in this ongoing fight. Presumably, child pornographers are using P2P to locate, download, and share sexually explicit videos and pictures of small children because they feel that they cannot be caught on such a disparate network. Tiversa pioneered the research and tactics used to track and catch these individuals. We are also currently training all levels of law enforcement nationwide through the FBI LEEDA program and have been seeking to work more extensively with other law enforcement and prosecutorial organizations.

Tiversa has used its ability to locate available files and track individual's P2P network searches to document cases where child pornographers and predators are actively searching P2P networks for personal photos of children and others that may be stored on private computers. Once the photos are downloaded and viewed, these individuals will use the "Browse Host" function provided by the P2P software which allows the user to then view and download all additional information being shared from that computer. If personal photos are being shared, it is most likely that the computer will also be sharing other personal, private information such as a resume or tax return. This accompanying information can be used by the predator to locate the address, telephone, workplace, etc. of the potential victim. Individuals at Tiversa have directly assisted in the investigation of these specific types of cases.

Sources of the Breach – Many individuals at this point would consider themselves immune to these types of identity theft and fraud if they never used or downloaded P2P software. This is not an accurate assumption.

In research involving over 30,000 consumers, Tiversa found that 86.7% of the individuals whose information was found on the P2P networks, were breached by a third party. Many of these individuals had their information exposed by their doctors, lawyers, hospitals, accountants, employers, banks and financial institutions, payroll companies, etc. Organizations that had a right to have access to the information were predominantly the source of the breach.

In the 60 day research period (2/25-4/26/09), Tiversa downloaded 3,908,060 files that had been inadvertently exposed via P2P networks. This number is only comprised of Excel spreadsheets, Word documents, PDFs, Rich Text, Emails, and PST files. This number does not include any pictures, music, or movies. It is important to note that these files were only downloaded with general industry terms and client filters running. Many more exist on the network in a given period of time.

Corporations and businesses

As a matter of record, Tiversa observes searches similar to those previously illustrated for "credit card" and for "medical" for individual corporate names, subsidiaries, and acronyms. The illustration of specific search strings in this testimony would put these corporations at further risk. General search terms include company names in combination with "confidential," "executive," "payroll" and other terms clearly designed to identify files containing important or personal information. The Committee should note that the searches of this nature are every bit as aggressive and more specific than those for credit cards and medical information – the larger and better known a company and its brand, the greater the risks associated with the searches for these corporations.

Corporate information disclosed on P2P networks includes breached PII and personal health information (the basis for much of the personal information used in identity theft described above), intellectual property, strategic documents and business plans. We have identified disclosures of legal documents, performance reviews, Board minutes, merger and acquisition plans, plant physical security plans, network diagrams, user ID's and passwords. Specific examples of inadvertent disclosures are described below.

One Supplier affects Thousands – In one instance, we identified one small company with fewer than 12 employees that provides third party billing services to hospitals. An inadvertent disclosure on patients from three different hospitals by this company exposed personal health information (patient names, SSNs, diagnosis codes, physician names, and other information) involving:

- 20,245 Patients
- 266 Physicians
- 4,029 Employer Organizations
- 335 Insurance Providers

It is easy to see the criminal value of the information exposed in this single breach and the potential impact to a broad range of individuals, professionals and organizations.

Corporate secrets revealed – In another instance, Tiversa discovered the PST file of a high-ranking officer involved in the merger and acquisition area of a Fortune 100 company. The entire Microsoft Outlook information of this officer was exposed to the public:

- Entire calendar
- Schedule of conference calls with dial-in numbers and passcodes
- Business and personal contacts including names, e-mails, addresses, phone numbers, etc.
- Over 12,000 e-mails to and from the individual
- Over 400 e-mail attachments (documents, PowerPoints, spreadsheets, etc.) including:
  - Regional sales information
  - M&A business integration updates
  - Strategic business alliances
  - Revenues through acquisitions

In the wrong hands, this information could be used for individual profit from trading on “insider information” not formally reported by the company, or on a much larger scale to manipulate and undermine the credibility of the capital markets.

Government, the Military and National Security

This risk also extends to the military and to overall national security.

Troop PII exposed – Tiversa has documented the exposure of the PII of men and women in the Armed Forces with frightening regularity. Military families are prime targets for identity theft as the thieves are aware that the soldiers are probably not checking their statements or credit reports very closely due to the serious nature of the work that they are performing. We have seen the confidential information (SSNs, blood types, addresses, next of kin, etc.) of more than 200,000 of our troops.

Classified information searched for…and found – P2P networks also pose a national security risk. In monitoring the origin of the searches on the P2P networks regarding national security issues, it is clear that organized searching is occurring from various nations outside the United States to gain access to sensitive military information being disclosed in this manner.

Searches are directed at identifying and obtaining sensitive information on matters of security using terms such as:

- Classified
- Military classified
- Military confidential
- Top secret
- US Marines classified
- Restricted

Examples of information breaches emanating from P2P networks and known to the public are described below.

In February of this year, Tiversa identified an IP address on the P2P networks, in Tehran, Iran, that possessed highly sensitive information relating to Marine One. This information was disclosed by a defense contractor in June 2008 and was apparently downloaded by an unknown individual in Iran.

On April 22, 2009, the *Wall Street Journal* printed a front cover story reporting that former Pentagon officials had indicated that spies had downloaded plans for the $300B Joint Strike Fighter project. Highly sensitive information regarding the Joint Strike Fighter program was also discovered on P2P networks.

Recommendations

For several years, Tiversa’s focus has been working with corporations and government agencies to mitigate P2P disclosures and risks. Based on our experience, we believe that there are steps that can help significantly decrease the likelihood of inadvertent disclosures and therefore increase the safety and protection of those most affected, the consumers. We humbly and respectfully provide the following recommendations for your consideration.

Increase Awareness of the Problem

Corporations are just becoming aware of the problem that the P2P poses to its information and data security. Individual consumers are even less prepared for the security threats that it poses. It is very difficult to protect against a threat that you are unaware of.

FTC – On the FTC’s website on the page “About Identity Theft,” there is not a single mention of P2P or file-sharing as an avenue for a criminal gaining access to a consumer’s personal information. Of the 6 methods identified on the website, very few if any could ever result in the consistent production, let alone the magnitude, of PII like the P2P networks.

Clearly, victims of identity theft must be educated and notified that P2P could be the source of their stolen information.

SEC – Awareness should extend to corporations and government agencies as well. Corporations regularly breach personal information of individuals (employees, customers, etc.). With consumers increasingly being asked to provide PII to employers, banks, accountants, doctors, hospitals, and government agencies, the recipients of this PII must be knowledgeable in the threats that P2P can pose to the security of that information.

Corporations also disclose non-public information that could be used for individual profit or to manipulate or undermine the markets. P2P risks and vulnerabilities that lead to these disclosures should be addressed in the application of current laws (Sarbanes-Oxley, Gramm-Leach-Bliley, etc.).

Federal Data Breach Notification Standards

41 of the 50 states have now enacted some form of data breach notification law. However, the laws vary from state to state and, in our experience, are seldom respected or followed by organizations. In some cases, companies that seek to do the right thing are unfamiliar with the various laws that may apply to their situation or have difficulty in complying with the applicable laws.

Standardized breach laws should be enacted to provide guidelines for any organization, public or private, that houses consumer or customer PII in the event of a breach of the information. In this regard, we believe that P2P risks and vulnerabilities should be addressed in the application of current laws, and we support HR 2221 – the Data Accountability and Trust Act. This proposed legislation requires the establishment and implementation of policies and procedures for information security practices and includes notification and remediation provisions in instances of breach.

The breach laws will also need to be enforced. Many disclosing companies disregard the current state laws, if any, to the severe detriment of the consumer whose information was exposed.

Any breach involving the release of a consumer's SSN should include mandatory identity theft protection for that individual for a minimum of 5 years. The often reported 1 year of credit monitoring is completely inadequate remediation for a consumer whose SSN was breached. Identity thieves will wait for the credit monitoring to expire after the year provided to begin to attack the consumer. This is supported by actual files Tiversa has seen with expiry tags entered directly into the filename and meta-data.

Military Personnel & National Security Disclosures

DOD – The safety and identity of our men and women in uniform of Congress should be vigorously protected. Measures should be taken to safeguard personal information, and to monitor, detect and remediate any disclosures. For soldiers who have had their information disclosed, comprehensive identity theft protection services should be provided to prevent and guard against the use of the breached information.

DSS – P2P networks should be continuously monitored globally for the presence of any classified or confidential information disclosed by defense contractors or subcontractors that could directly or indirectly affect the safety or security our citizens.

Consumers

Tiversa also suggests the following recommendation for consumers:

Know Your PC (and who is using it) – Parents need to pay close attention to the actions of their children online, especially when the children are using a shared PC with the parents.

Just Ask! Consumers need to ask anyone who is requesting their PII (doctor, hospital, lawyer, banking institution, accountant, employer, etc.) what protections that the organization has in place to protect against inadvertent disclosures on the P2P networks.

Consider Identity Theft Protection Service – Organizations offer a wide variety of services to help with identity theft from credit monitoring to the more proactive placing of fraud alerts and black market monitoring. Consumers should select an ID theft protection service that offers proactive monitoring and remediation of P2P related disclosure.

Conclusion

In conclusion, the inadvertent file sharing through P2P File Sharing networks is highly pervasive and large in magnitude. It affects consumers, corporations of all sizes, and government agencies.

Existing policies and IT measures have not been effective at preventing information from becoming available. Malicious individuals regularly use P2P file sharing networks to obtain sensitive, confidential, and private information. They pose an immediate threat to national security, business operations and brands, and consumer fraud and ID theft.

The Committee should seek to create broader awareness of the problem. It should encourage individuals, corporations, and government agencies to continuously audit P2P networks themselves to enable these entities to intelligently determine their exposure and to design strategies to mitigate their issues.

Mr. Chairman, taking these steps will better protect us all from the dangers that lurk in these networks while allowing for legitimate uses of this powerful technology in the future.

Thank you for the opportunity to testify today.