



# ParetoLogic Privacy Controls

Uncovering the Ghost in the Machine

Product White Paper  
December, 2009



# ParetoLogic Privacy Controls

---

**ParetoLogic Privacy Controls** provides easy and efficient methods of finding and erasing unwanted and unnecessary items on your computer. With Privacy Controls you can erase items that are created automatically and are temporarily cached on your system. This frees up space on your hard drive and improves computer performance.

To get a free scan, check out: [www.paretoLogic.com](http://www.paretoLogic.com).

## ParetoLogic – The Company

ParetoLogic is an international software development company headquartered in Victoria, British Columbia, Canada. We specialize in providing advanced security applications and performance tools for business and personal computer users.

ParetoLogic creates solutions that combine sophisticated technology with a truly user-friendly interface. Our products empower people to secure and optimize their computers and are available in eight languages in 70 countries around the world. ParetoLogic has established partnerships on a global scale to make our products available to all computer users regardless of location, language, or computing experience.

We provide attention to your needs and we are committed to delivering exceptional software applications and resource-rich web sites. Our solutions will exceed your expectations.

© 2009 ParetoLogic Inc.



# ParetoLogic Privacy Controls

## Addressed in this Product White Paper

This paper includes the following:

Unwanted and non-secure items on our computers	4
- A brief history of the build up of unwanted items on computers	4
- Present day concerns; clutter and recent activity information	6
- Security concerns	8
Deletion	9
- “Deleting” and Data Remanence	10
- Overwrite Technology	11
ParetoLogic Privacy Controls	11
- Scan & Erase	11
- Advanced Shred	13
Looking Forward	14
Security and Peace of Mind	15

This document provides information related to ParetoLogic Privacy Controls. It is not meant for instructional purposes. We recommend using the help file that comes with the application for detailed steps and instructions.



# ParetoLogic Privacy Controls

## The Ghost of Computer Past

In an online article<sup>1</sup> entitled: “Hard Drives Exposed”, PC World describes salvaging ten used hard drives. Of the ten drives, all except one had sensitive business or personal data remaining. In another independent study<sup>2</sup>, it was discovered that of 200 drives purchased on eBay, 113 had confidential data remaining on them. This paper speaks to the accumulation of unwanted and sensitive data and methods of removal and erasure.

### The Accumulation

Having sensitive data on our computers is not surprising considering the reliance of computers in our present day-to-day lives. The history of personal computing has not been a long one. In the mid-1980's Apple (and Microsoft shortly afterwards) released the first home computer with a graphical user interface. By the mid-90's personal computers were considerably more attainable. Ten years later, a radical transformation has occurred and shaped our computing experience. Being online is a commonly understood and an integral activity. The reasons for this transformation include:

- Lower cost and increasing availability of the technology (computers, hardware, software, Internet access, online kiosks, cybercafés, etc.)
- Greater familiarity with the technology; easier to learn and operate
- Growing financial and business use including investment, entrepreneurship, and other activities related to e-commerce; computer use and computer networking in the office-place is common practice
- Increasing exposure to computers through Internet and media coverage
- An increase in computing activities: games; multi-media such as images, video, and audio; information sharing and online communications including newsgroups, online chat rooms, instant messaging, and of course email

---

<sup>1</sup> April 2003 (web site: [http://www.pcworld.com/article/110012/hard\\_drives\\_exposed.html](http://www.pcworld.com/article/110012/hard_drives_exposed.html))

<sup>2</sup> May 2005 (“Data Data Everywhere 2005”, Olaf Kehrer, O&O Software, Berlin)



# ParetoLogic Privacy Controls

- An increase in product offerings as well as cross-over and compatible mobile technologies such as Internet capable cell phones, Internet watches, PDA devices, notebooks, laptops and more

This is but a small sampling of the technology on hand. The effects of the transformation have been equally vast. In essence, we have gone from a closed-system of personal computing to a world-wide online connection. In the early to mid 1990's, if there was a computer in a household, the functionality was limited; there were fewer avenues of online connection, and likely one-user-to-one-computer access.

Now, home computing involves sharing computers amongst several users. This could mean establishing accounts or using the same user account, setting up a network with more computers in the home or an office setting, having high speed Internet access, taking advantage of wireless connections, and hooking into online activities so as to be connected to millions of computers worldwide. This is not simply a North American phenomenon. As of December 2005, there were 158 million broadband subscriptions throughout OECD countries (Organization for Economic Cooperation and Development). With respect to penetration, Iceland, Korea, the Netherlands and Denmark take the lead with more than 1 out of 4 inhabitants having a connection to the web.<sup>3</sup>

In the mid 1990's, computing technology did not take certain considerations in to account that are today a necessity to maintain security and protection. For Microsoft Windows users, we can imagine scenes displayed to us from the ghost of computer past that include temporarily stored files, caches of unused items, and operating systems weaknesses and glitches that will in time expand to become security holes. What does this mean for us in present day computing reality?

## The Ghost of Computer Present

Our appetite for online activities is nothing short of expansive and bordering on gluttonous. In the midst of our online consumption there is security risk and performance degradation. Clutching at the feet of the mammoth giant known to us as today's Microsoft computer experience are the often unnoticed contributors to performance and security: clutter and recent activity information. While clutter can slowly choke a system, it is best to beware of recent activity information.

---

<sup>3</sup> From: "Internet Statistics and Reports" (web site: <http://www.netcaucus.org/statistics/>)



# ParetoLogic Privacy Controls

## Clutter

Simple daily use of your computer can lead to the build up of clutter – unwanted items left behind and unused. Running programs and using the Internet leads to data being stored on your hard drive and items placed in your registry. Caches, temporary files, and “deleted” items are good examples of clutter.

A cache (pronounced "cash") is a temporary store of information that has been duplicated for the purpose of speeding up access so as to reduce bandwidth usage and server load. When browsing web sites, your system stores a cache of viewed files in temporary folders. These can be accessed on subsequent visits to the site so as to speed up the display of content or so that the content can be viewed offline. Over time these temporary stores of content build up unnoticed and can eventually weigh down a system like the chains of Jacob Marley's ghost.

High-speed browsing and ever-increasing amounts of content on web sites are conditions that lead to a quick build up of clutter. Too many unwanted files on your system can bring about a reduction of hard drive space, poor performance, and issues with applications. Along with temporary files stored in Temp directories, “trash items” are another example of clutter – unwanted files that remain on your system.

Similar to Internet caches, applications create and access temporary files for short-term computations, to save time, or to uncompress files. In these situations using RAM is not an option as it would only be stored until the next reboot or because the item is too large to store in RAM. Creating a temporary file is done in much the same way we would write a note to ourselves and leave it on the desk as a reminder. It can be left indefinitely and can take up valuable space. In some instances, developers of these applications could have programmed the means to delete these temporary files but have not done so. In many instances these items can be safely removed.

There are other items on your computer that have been “deleted” but in fact are stored in a separate container or folder by the application or the system. Examples of this include the system “Recycle Bin” and the “Deleted Items” folder in email applications. You can restore the item or choose to permanently delete it so as to not access it again using the application or Windows Explorer. However, these files can be recovered using non-conventional means as described in this paper (see: “In The Machine” on page 9 for more).



# ParetoLogic Privacy Controls

## Recent Activity Information

Current technological advances include offering pointers and history items to direct you to recently used locations and files. When you type the first letters of a web site address, the Browser offers a list of previously viewed sites as a way of auto-generating the URL. These items are stored in memory and offer you a reference point. The following table includes some examples.

Type	Description
History	Computer applications often keep a history of previously opened or viewed items to offer quick access to recently accessed files. For example, web browsers store links to recently visited web pages and previously viewed web sites are displayed from history panes.
Pointers	Applications store an address location in memory to save time and effort typing in or locating the address again. For example, when you open the Save As dialog it opens to the location of the last saved item.
Cookies	Cookies are files that are stored on a computer system after viewing a web site. There are cookies that store information such as username and password so that you do not have to enter these every time you visit the site. Cookies can also be used to track browsing activities across multiple web sites. Often this is done to present the user with specific advertisement to entice them to buy. As a result, privacy and security of information are at risk.
Logs	Logs are files containing information for the purpose of record keeping. Applications offer the option of storing communication logs (for example, chat logs). Some applications automatically create data logs to record events. In this way they can diagnose problems and offer technical support.

Table 1: Types of Recent Activity Items



# ParetoLogic Privacy Controls

## Security - The Real Score

Security of personal and financial information is severely compromised when traces such as those listed in Table 1 are left on your computer. Windows operating system and Browser vulnerabilities are rampant. Internet Explorer 6 is a good example. Despite known vulnerabilities, Microsoft has not fixed security flaws promptly and in some cases, not at all. According to security reports<sup>4</sup> there were 106 security advisories (vulnerabilities) for Internet Explorer 6.

Internet Explorer uses component architecture (COM: Component Object Model), permits third party applications to add functionality using Browser Helper Object (BHO) technology, and allows ActiveX content for web sites that wish to add rich content. Creators of “malware” (malicious software including viruses, adware, and spyware), have taken advantage of these security flaws. Users can receive malware unknowingly simply from viewing web sites; they become a victim of a “drive-by download”.

Some types of malware that are designed to collect information for malicious activities include the following:

Type	Description
Adware	Display unwanted or intrusive ads and covers a broad range of threats. For example, they can display ads in Browser windows, open commercial web sites, and collect data for market research.
Exploit	Exploit security vulnerabilities in other programs often to allow an intruder to remotely access the computer.
Trackware/Data Miner	Track web usage, web searches, or general computer use. Cookies are one kind of data miner, some of which attempt to collect private information.
Spyware/Surveillance	Designed to collect data for a variety of purposes, true Spyware (or surveillance) applications record personal or private

<sup>4</sup> From: Secunia ([www.secunia.com](http://www.secunia.com)), Oct 05, 2006



# ParetoLogic Privacy Controls

	information and transmit it to a third party. Often this data is used for market research and advertising, but more malicious programs attempt to steal passwords and login information, banking details, and credit card information.
Browser Helper Object (BHO)	BHOs are not inherently dangerous. They are DLL files that are executed by Internet Explorer. Add-in toolbars and sidebars are BHOs and many of them are completely benign. However, a great number of BHOs function maliciously in that they track web usage, record private data, and even display ads.

Table 2: Malware Security Threats

New classes of viruses are created as the sophistication and methodology of malware evolves. In a recent article by globeandmail.com<sup>5</sup> a new class of viruses called “ransomware” was brought to light. A security vendor named one such offender “Troj/Ransom-A”. According to the article, ransomware takes control of your computer system and asks for a ransom in exchange. Although uncertain how it spreads (drive-by-downloads or spam), once a computer is infected, the Trojan proceeds to freeze system functionality and demands a ransom be paid using a transfer service. In true hostage fashion, files are threatened to be deleted every 10 minutes unless \$10.99 (U.S.) is paid. It was not mentioned in the article if these files are deleted to the Recycle bin.

## In The Machine

Security from known and ever-emerging online threats is an increasing concern. Keeping our information secure demands awareness of what our computer system is and is not doing. For example, when “deleting” a file within a Microsoft operating system the file is placed in the Recycle bin. It remains there until you restore the file or empty the Recycle bin. Even after deleting it from the Recycle bin, the actual data remains on the hard disk storage medium.

<sup>5</sup> “Trojan freezes computer, requests ransom” posted 10:22 am EDT on 01/05/06



# ParetoLogic Privacy Controls

## “Deleting” and Data Remanence

Even when removing items from the Recycle Bin, the data is not in fact erased. Imagine it as having a line removed from the table of contents of a large book. You can no longer look up the name of the item, refer to the page number and locate the information. However, the pages remain buried within the book.

When emptying the Recycle Bin, the Microsoft system designates files as deleted using a special character and you can no longer access the file information. However, what the system does not do is remove the data that is stored on the disk drive. What is removed is the reference to the data. The data is on the drive but it simply cannot be accessed using standard means. Recovery tools can perform low level scans to locate files. This is essential to data recovery and in understanding how to alter data stored on disks so as to make them unrecoverable.

Data remanence is the term describing situations where residual data remains on the storage device after some deletion has been performed. Care should be given to understanding what happens when using common means of data removal. For example, it is thought that formatting the hard drive wipes the disk so you are starting with a fresh drive. However, unless special options are applied, a standard format command (referred to here as a “high-level format”), in fact erases the root directory entries. Once again, data recovery tools can be applied in these instances to recover the data.

Often users will format their computer system before selling their computer or to get a fresh start for a computer system that may be overly plagued with an excess of files or malware. If the reformatting or erasing is not done properly, data remains when rebuilding the system; users risk having personal, financial, or business data ending up in the wrong hands.

Organizations such as the National Security Agency and Department of Defense have placed considerable effort toward data remanence issues and have adopted methods of “sanitization” and “redaction”. A classic example of insufficient care not being utilized in a sanitization process involves a US military report. In this case the report dealt with information related to the death of an Italian secret operative, Nicola Capilari. In May of 2005, the file was publicized in Adobe pdf format with sensitive information blacked out. It was soon discovered the data could be revealed using cut and paste procedures.



# ParetoLogic Privacy Controls

## Overwrite Technology

As can be surmised, once you create and save data, the stored data is considerably persistent. Common methods of deletion are limited to the removal of common means of connecting to the saved data. The data remains stored on the hard disk until it becomes overwritten. This has been a known issue as early as 1960. It was recognized that sensitive information could be disclosed if proper and effective procedures to remove data were not employed.

There are two ways to ensure destroying data: low-level formatting and using overwrite technology. Low-level formatting is performed in a DOS environment and involves permanent removal of data on your drive. This is the solution to take when reformatting (wiping) your system – including any form of malware. However, it is not practical for removal of sensitive information on a day-to-day basis.

Overwrite technology involves the act of recording new data overtop existing data. For example, ParetoLogic Privacy Controls utilizes overwrite technology that involves replacing byte information with all zeroes, all ones, a random pattern, or a combination of these depending on the overwrite level that is selected. The data that is overwritten is non-retrievable – it cannot be restored.

## ParetoLogic Privacy Controls

ParetoLogic Inc., an International software company, has developed and made available an erasure program that offers removal of clutter and unwanted items, and has included the ability to select files and have them “shredded” using overwrite technology.

The following table depicts the different erasure options available:

Type	Erasure Option	Uses
<a href="#">Scan and Erase</a>	- Secure Delete - Shred levels	The Scan and Erase is used as an automated way of detecting clutter and unwanted items. It is capable of quickly detecting numerous unwanted items on your computer including system, application, and registry items.



# ParetoLogic Privacy Controls

<a href="#">Advanced Shred</a>	- Shred levels	The Advanced Shred tool is used to manually select and permanently erase files from your system.
--------------------------------	----------------	--

Table 3: ParetoLogic Privacy Controls Erasure Options

Choosing the type of erasure that suits your needs depends largely on the items you want to erase and the capabilities of your system. In some cases a scan will detect thousands of items. This could take some time if using several overwrite passes. The following diagram depicts the levels of erasure and the types of files that could be securely deleted or shredded.

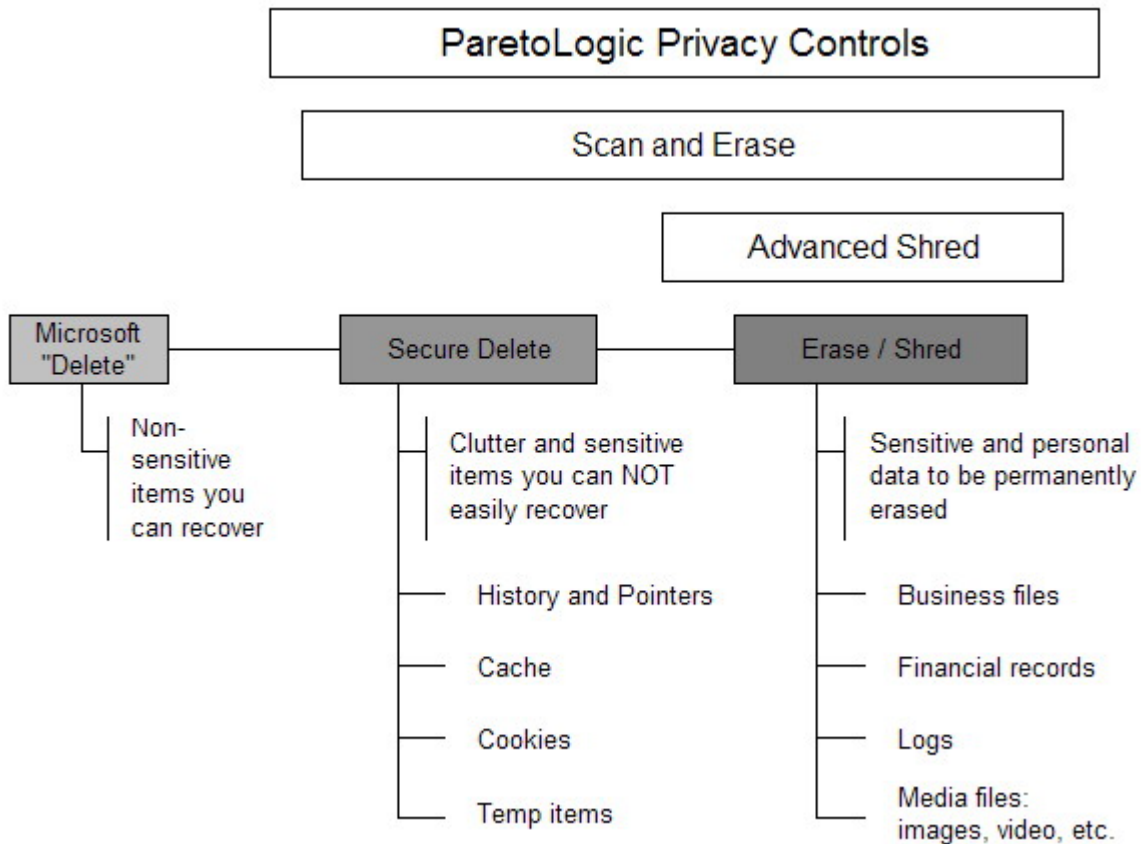


Diagram 1: Delete – Erase Continuum



# ParetoLogic Privacy Controls

## Scan and Erase

The Scan and Erase tool is designed to deal with clutter and unwanted files left on your system. You can scan your system and supported applications for unwanted items. You can choose to securely delete these items or you can have them shredded using one of the Shred levels.

## Advanced Shred – Permanently Erasing Files

With ParetoLogic Privacy Controls you can also shred sensitive files that you would like permanently erased. All data on your computer is comprised of "bytes" of information based on a binary numeric system. Each byte is comprised of zeroes and ones (for example, 00111001). The Shred tool uses overwrite technology – a method of replacing the stored data with another set of numbers. Typically this is all zeroes or a random set of zeroes and ones. The Shred levels are as follows:

Shred Level	Security	Description
Quick	Minimum	Data is overwritten with a single random pass and cannot, without the use of sophisticated restoration equipment, be recovered.
Safe	Medium	The data is overwritten in three passes according to DoD 5220-22M specifications (the standard for permanent erasure of digital information as set by the U.S. Department of Defense). This is the recommended setting as it meets security requirements without over-extending system resources.
Thorough	High	The data is overwritten according to DoD 5220-22M specifications (the U.S. Department of Defense standard), but includes an extra four passes for a total of seven. This is very secure but will take more time especially when shredding many files at once.

Table 4: Types of Shred Levels



# ParetoLogic Privacy Controls

## Our Computer Future

In general terms, computer technology of the future is to be smaller, faster, and anywhere. In effect, microprocessors could be built into furniture or woven into fabric. Intel's fourth generation laptop platform will include several gigabytes of flash memory and their multi-core technology (the combination of integrated execution cores) is underway as prototype chips with eight cores have been developed. Gigabytes of storage will make way for terabytes and roll up screens will be available for laptops.

What about the PC? What does the future hold for it after 25 years of dominating the digital world? PCWorld<sup>6</sup> published predictions on what devices would most likely have mass appeal in 2011. Portable game consoles were the long shot followed by media players and Ultra Mobile PCs (UMPCs). Smart Phones will continue to have mass appeal, but at the top of the list is the PC. A desktop, laptop, or tablet PC will be the "...primary device for work or play".

What about security – will it keep up? Some time around the turn of the millennium there was greater exposure and resulting acceptance of online financial transactions. As many of us entered our credit card information online for the first time, we took greater notice of security of information. Those of us who have received unwanted spam, adware, or malicious software have placed considerable effort in restoring and maintaining our privacy and reducing system vulnerabilities and weaknesses that permit these intrusions. A requirement of participating with online conveniences is trust.

In January of 2002 Bill Gates sent out a company email memo mandating a shift from a feature-rich focus to security and privacy. The memo pushed for a sea-change of programming, to create software and operating systems that would preclude security risks and any worries from the user. It is obvious that this has not happened yet.

The uphill battle here is that storage of data is intrinsically permanent. Add to this that malware is becoming more sophisticated and the fact that we are connecting to others around the world, it is clear to see that these issues of security and privacy are both global and common.

---

<sup>6</sup> PCWorld.ca (<http://www.pcworld.ca/news/column/8559e8f00a01040801c7c7c37338ea00/pg1.htm>) "The future of your PC: One device to rule them all?"



# ParetoLogic Privacy Controls

A lesson from the past is essential... as early as 1960 the retentive properties of storing data was recognized. Data removal procedures were required to prevent inadvertent disclosure of personal and sensitive data. The future of computers will continue to be expansive. Being equipped with the right tools is essential to protecting one's security and privacy.

## Security and Peace of Mind

Dealing with computer performance and security issues is of prime importance from a business, financial, and personal home-use perspective. Leaving traces of your computing activities and having personal information accessed without your consent can have many ramifications from loss of privacy to being the victim of criminal activities.

ParetoLogic Privacy Controls is a dedicated software solution that provides proficient means of erasure and gives you peace of mind. Having seen the ghosts in the machine, the clearest course of action is to use an informed choice and to make the change.

*All information contained in this document is the proprietary information of ParetoLogic Inc. and is protected by international copyright treaties. This document contains information that is privileged and confidential. Any disclosure, distribution or copying of this document without the prior written consent of ParetoLogic is strictly prohibited under applicable law. ParetoLogic and ParetoLogic Privacy Controls are registered trademarks or trademarks of ParetoLogic Inc. in Canada, the United States, and in other countries. All other trademarks are the property of their respective owners.*

*Copyright © 2009 ParetoLogic Inc. All rights reserved.*