



**AccessData®**

*A Pioneer in Digital Investigations Since 1987*

AccessData Corporation

# Using SilentRunner in Compliance with EU Privacy Laws

White Paper

Jason Mical, Director of Network Forensics  
12/5/2008

## **Table of Contents**

<b>Background</b> .....	1
<b>The Product</b> .....	1
<b>The Privacy Laws</b> .....	2
Article 8 .....	2
Article 10 .....	2
OECD Guidelines .....	3
<b>Application of SilentRunner to Meet the Principles of the EU Directive</b> .....	4
<b>Getting Started with SilentRunner</b> .....	5

---

## Background

As technology has advanced to include the capabilities to monitor networks and view individual transactions on all forms of networks, including the internet, the European Union (EU) and its member countries have become increasingly concerned about the privacy of the individual. The EU has passed directives outlining the guidelines that law enforcement, governments and corporations must follow regarding what can and cannot be done. In addition, each of the member countries have passed laws that use these guidelines as a base, but adapt these as they feel meet the needs of their citizens.

AccessData has developed a software tool that gives the user the capability to monitor networks, analyze logs, do post event forensics, see data or information leakage, and monitor individual activity on email, the internet, or instant messaging. While many of the firms throughout the EU would like to utilize this tool, their legal departments have blocked the usage because they fear it would violate the privacy laws of their respective countries. However, this tool has been widely used throughout Europe by various governments to assist in forensic investigations, and by corporations to analyze logs and set firewall rules to prevent unauthorized attacks on their corporate networks.

The purpose of this white paper is to describe how this product, SilentRunner, can be successfully used to assist corporations without violating EU privacy laws. It has been reviewed by legal teams and corporate privacy experts to ensure that we are as complete and accurate as possible. This paper is intended to be distributed to legal departments of corporations across the EU to illustrate the capabilities and controls of SilentRunner that allow organizations to utilize this solution in compliance with privacy laws and guidelines.

## The Product

SilentRunner was first developed by Raytheon Corporation and known as Silent Runner. It was sold extensively to governments around the world to better understand what was happening on their networks. With the proliferation of the internet and the growth of large corporate networks, the product was sold to both government and commercial organizations. It can be used in both a real-time and post-real-time mode. If used in a real-time mode, it sits on a span port of a network segment and monitors the packets or network traffic that crosses that network segment. It has the ability to view everything that crosses that network segment, including email, instant messaging and traffic going to the World Wide Web. It is this capability that must be controlled, or used only in extreme cases with the consent of appropriate parties.

Utilizing the product in a post-real-time mode to analyze the logs of other security tools to determine what occurred or to monitor the network without being able to view personally identifiable information (PII) is permitted in most countries.

To be a little more technical, when the product is being used in a monitoring mode, much like a sniffer, it has the ability to monitor IP addresses, showing where they are communicating. The system creates two types of logs:

- Transaction logs simply show the communication of the header information, without being able to view the contents of the message. In other words, it will show that IP address 140.145.40.210 communicated with IP address 149.146.40.247, and nothing more. When using transaction monitoring, only header information is visible—no PII or message contents.
- Session logs are created when the solution is used to monitor payloads or content. This is done by turning on the session capture capability, which then collects all of the content associated with the transmission of that message. It is this feature that potentially conflicts with EU privacy laws, as legal departments are concerned that the operator of the system could randomly turn on this capability and view private messages.

## The Privacy Laws

The base for the privacy laws comes from the European Directive 95/46 EC which lays out the provisions under the European Convention for the Protection of Human Rights and Fundamental Freedoms. Each of the member countries can take this directive as the base and pass national laws that meet the needs their citizens. There are two articles which explicitly state the goals of the directive, Articles 8 and 10. They are summarized as follows:

### Article 8

1. Everyone has the right for respect for his private and family life, for his home, and his correspondence.
2. There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interest of national security, public safety, or the economic well being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection or the rights and well-being of others.

### Article 10

1. Everyone has the right to freedom of expression. This right shall include the right to hold opinions and to receive and impart information and ideas without interference by public authorities and regardless of frontiers. This article shall not prevent states from requiring the licensing of broadcasting, television or cinema enterprises.
2. The exercise of these freedoms, since it carries with it responsibilities and duties, may be subject to formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interest of national security, territorial integrity or public safety for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or the rights of

others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

## OECD Guidelines

Much of the work and information that AccessData will follow when putting forth our implementation using SilentRunner in compliance with the European Privacy directives and laws is derived from guidelines set forth by the Organisation for Economic Co-operation and Development (OECD), the *OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data*. We are not addressing the Trans-border Flow of Personal Data in this white paper, but instead are focusing on the Protection of Privacy and how we would comply with these guidelines. Specifically, we will focus our efforts on Part 2 of the following description of the Guidelines: Article 23. The Guidelines set out in the Annex to the Recommendation consist of five parts. Part One contains a number of definitions and specifies the scope of the Guidelines, indicating that they represent minimum standards. Part Two contains eight basic principles (Paragraphs 7–14) relating to the protection of privacy and individual liberties at the national level. Part Three deals with principles of international application, i.e. principles which are chiefly concerned with relationships between Member countries.

The basic principles for data privacy as defined by OECD and applied in the EU are as follows:

- 1. Collection Limitation Principle**  
There should be limits to the collection of personal data.
- 2. Data Quality Principle**  
Personal data should be accurate, complete and kept up- to-date.
- 3. Purpose Specification Principle**  
The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
- 4. Use Limitation Principle**  
Personal data should not be disclosed, made available or otherwise used for purposes other than those specified.
- 5. Security Safeguards Principle**  
Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.

## **6. Openness Principle**

There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.

## **7. Individual Participation Principle**

An individual should have the right:

- a) To obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him;
- b) To have communicated to him, data relating to him
- c) to be given reasons if a request made under subparagraphs(a) and (b) is denied, and to be able to challenge such denial; and
- d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or amended.

## **8. Accountability Principle**

A data controller should be accountable for complying with measures which give effect to the principles stated above

## **Application of SilentRunner to Meet the Principles of the EU Directive**

We have chosen to take a strategy that will give each organization within each country the ability to select the level of accountability they wish. In other words, in countries such as France and Belgium, the privacy laws take on a very stringent interpretation. Even to be able to sell into France, except for Law Enforcement, AccessData must apply for a license to sell in the country. Then each potential customer must also apply to the Interior Ministry for a license to be able to monitor their networks or communications. Other countries, such as the United Kingdom, have taken the position that as long as they disclose that they are monitoring, they have the right to protect their business and network.

AccessData has a product called the SilentRunner Privacy Option, which will meet even the most stringent laws, because it takes out the ability to collect content or session decoding. This capability is not included with the system and cannot be turned on. This will give the company the ability to see the traffic transverse the network, but will not be able to determine who the communication came from or what was included in the transmission. The system will be able to monitor the traffic patterns that occur on the network (often called electronic discovery), showing, for example, that IP 140.20.18.195 communicated with IP 140.20.20.180, but not who it is or what was said, so that no PII can be detected. This option also includes the ability to correlate logs from other security devices, and visualize the results on a screen. It also can work with other security devices, such as firewalls, to ensure that the rules are set correctly. This option would act like a sniffer, but better meet the privacy laws, because no content has been collected.

Using the full product as it exists today gives the operator the ability to turn on or turn off the session decoding option, using a protected password. This password could be given to the Employee Representative, and he or she would be designated as the one with the capability of leading an investigation or turning on the monitoring capability when probable cause has occurred to warrant the monitoring of a given employee. In this case, like the Privacy option, the company would be monitoring its network, looking for abnormalities. If an abnormality is found, the Employee Representative would be called in and a determination would be made whether the infraction warrants further investigation or monitoring. This would be much like a search warrant, where the scope and timing of the monitoring would be set by the Employee Representative. In most cases, this is the method used by law enforcement agencies throughout the world, so that they cannot indiscriminately abuse their technical capabilities. They must have probable cause, and the parameters are set and closely monitored with respect to who they can monitor, what they can monitor for, how long they can monitor, and what is admissible or inadmissible.

## **Getting Started with SilentRunner**

An example of how SilentRunner can be validated by EU organizations that wish to use SilentRunner, while ensuring compliance with privacy directives, occurred in one of the member countries. The software was used to monitor the communications of several highly sensitive servers at a large client. The firm wanted to watch the communications to and from several databases and applications across their network. However, before starting the proof of concept, the General Manager set up a test to ensure that we could not monitor or see email session content. After showing that emails were traversing the network but were not showing up on the monitor, we were allowed to proceed.

In many firms, the ability to protect privacy by the use of the password will be sufficient. Others will require the authorization and approval of the Employee Representative. Some firms will want the ability to ensure that PII is not leaving a firm, and will want to monitor that fact.

Companies in the US are using the product to ensure that personal data, such as social security numbers or account numbers are not leaving the network. We are continuing to enhance the solution's compliance monitoring capabilities, so organizations in all countries can be certain they are doing everything possible to ensure the privacy of the individual. For those with the most stringent laws or regulations regarding privacy, the Privacy Option can be purchased, which cannot be used to monitor email, chat or web communications. Should that capability be desired, the firm would have to purchase an upgrade and have AccessData install a new version of the software.