MTBN.NET PLR Library
Category: Business File: Beating_Crime_with_Printers_utf8.txt
Text and Word PLR Article Packs available at PLRImporter.Com

Title:
Beating Crime with Printers

Word Count:
757

Summary:
Perhaps it would be naive to think that the 21st century governments would stop at monitoring your every move on the street. Pause for a minute to contemplate what the next level of tracking could include. The answer is laser printers. If you think a document from your colour laser printer doesn't carry your name, think again.

Keywords:
laser printers, Xerox Corporation's DocuColor, laser printers, Electronic Frontier Foundation, EFF, inkjet printers

Article Body:
Perhaps it would be naive to think that the 21st century governments would stop at monitoring your every move on the street. Pause for a minute to contemplate what the next level of tracking could include. The answer is laser printers. If you think a document from your colour laser printer doesn't carry your name, think again.

The Electronic Frontier Foundation (EFF) claims that it has cracked the tracking codes embedded in Xerox Corporation's DocuColor laser printers. Such codes are simply one of the numerous ways manufacturers employ technology to help governments fight currency counterfeiting.

The United States government is allegedly involved with a number of other companies in separate anti-counterfeiting programmes meant to prevent currency from being scanned and printed. The U.S. government, however, is not the only country teaming with the printing industry to fight counterfeiters. A few experts believe that the Dutch government is also using similar anti-counterfeiting methods through Canon’s encoding technology.

Researchers in the U.S. have uncovered patterns of yellow dots arranged in 15 by 8 grids and printed repeatedly over every colour page. The dots, however, are visible only with a magnifying glass or under blue light, which causes the yellow dots to appear black. The code appears as a grid of microscopic yellow dots, each less than a millimeter in diameter. These millimeter-sized dots

appear about every inch on a printed page, nestled within the words and margins. By analyzing various test pages printed by supporters worldwide, researchers found that some of the dots correspond to the printers' serial numbers, and other dots refer to the date and time of the printing.

Consider two documents – one carrying the author's name and one meant to be anonymous. By comparing the codes, it can be determined whether the two documents were printed by the same printer, even if Xerox reveals nothing about a customer's serial number. The EFF is now studying printers from other well-known manufacturers with similar tracking codes, but whose keys remain secret.

Unlike inkjet printers, laser printers, copiers, and fax machines fire a laser through a mirror and series of lenses to embed the document or image on a page. Such devices range from a little over £80 to more than £1000, and are designed for both home and office use.

Peter Crean, a senior research fellow at Xerox, says the company pioneered this technology about 20 years ago because several countries had expressed concern about selling the printers in their country. The move aimed at allaying fears that their colour copiers could be easily used to counterfeit bills.

It is believed that since then, many other companies have adopted the practice. According to experts, several printer companies secretly encode the serial number and the manufacturing code of their colour laser printers and colour copiers on every document those machines produce.

Laser-printing technology makes it extremely easy to counterfeit money and documents, and the dots, according to supporters, in use in some printers for decades, allow law enforcement agencies to identify and track down counterfeiters.

However, the same dots could also be employed to track a document back to any person or business that printed it. Although the technology has been present for a long time, printer companies have not been required to notify customers of the feature.

If this practice disturbs you, don't bother trying to disable the encoding mechanism of your printer—you'll probably break it. The coding device is a chip located deep into the machine, near the laser. It embeds the dots when the document is about 20 billionths of a second from printing.

Although nobody has an estimate of how many laser printers, copiers, and multifunction devices track documents, experts believe that the practice is

MTBN.NET PLR Library
Category: Business File: Beating_Crime_with_Printers_utf8.txt
Text and Word PLR Article Packs available at PLRImporter.Com

commonplace among major printer companies. The U.S. Secret Service would agree that it finds the printing industry quite helpful to law enforcement.

According to sources, counterfeiting cases are brought to the Secret Service, which checks the documents, determines the brand and serial number of the printer, and contacts the company. Some, like Xerox, have a customer database, which they share with the government.

Many people are apprehensive that the American government’s tracking initiative could lead to a serious breach of privacy. The government has already succeeded in persuading more colour laser printer manufacturers to encode each page with identifying information. Without your knowledge or permission, an act you assume is private could become public. A communication tool you use in everyday life could become a tool for government surveillance. And what's worse, there are no laws to prevent its abuse.