Invasion of the Data Snatchers

A Puma Technology White Paper

April, 1999

Contents

Keeping Enterprise Data in its Place

Enterprises are on the verge of losing control of their data. The threat isn't from sheer volume of data, or from industrial espionage, although both those things can be problems. Instead, the threat comes from all those cute little mobile devices that were little more than toys a few years ago. Personal Digital Assistants, cell phones, and pagers can all increase personal and corporate productivity. But these small devices can also compromise corporate data. Left uncontrolled, they can become miniature repositories of corporate information comfortably tucked in the insecure pockets of individuals.

So, what's changed over these last few years to turn these innocuous devices into a looming threat? Until recently, small devices tended to be used as standalone tools for improving individual productivity. Instead of carrying a paper calendar, for example, a person could carry an electronic organizer or palmtop computer that was smaller yet served the same purpose. Most small devices produced before 1996 were primarily a convenient way to store personal information. Limited in memory, and difficult to program, these devices rarely held more than a small amount of personal data.

In 1996 the first mobile data snatcher was born. That was when Palm Computing—now part of 3Com—introduced the first device in what was to become the PalmPilot family. This device sported three compelling benefits that made it stand out from its predecessors. The first benefit was its extreme ease of use, which made it the productivity tool of choice for millions of users. The second benefit was its built-in connectivity, which made it easy to synchronize data between the device and a PC. The third benefit was the availability of excellent tools for creating new PalmPilot applications, including connectivity components for adding synchronization to those applications.

The PalmPilot charted the way for a new class of connected organizers. Such devices immediately began filtering into the enterprise, oftentimes masked as individual purchases that quietly appeared on expense reports. Despite the promise of these exciting devices, their built-in connectivity features make them serious risks to the integrity of enterprise data.

The threat these data snatchers pose demands action. Mobile devices are no longer limited to holding only simple personal information like addresses and schedules. They can now send and receive email messages, messages that may contain sensitive information. New utilities and toolkits extend the capabilities of the devices, allowing them to synchronize with any number of enterprise applications and databases. It's now quite possible for users to compromise enterprise data without even knowing it.

For companies that believe corporate data is a corporate asset, this situation is unacceptable. Some steps must be taken to prevent the "data chaos" that the unmanaged use of small devices can cause in the enterprise. Mobile devices are too valuable to ban outright. The challenge is to maximize and even extend the productivity benefits of these devices while minimizing the risks they pose for enterprise data.

It's time for a new breed of tools—tools that let an enterprise manage the ever-increasing number of mobile devices connected to its networks. Called *Mobility Management Tools*, these powerful applications can manage data snatching mobile devices, returning control of enterprise data to the company.

The Evolution of the Problem

Mobile computing began years ago with the introduction of the first portable computers. The widespread acceptance of notebook computers in recent years was Phase I of the evolution of mobile computing. In this *PC Connectivity* phase, it became clear that notebook computers could deliver real value to the enterprise, particularly when they had some level of access to corporate data.

Attempts to further reduce the size and cost of mobile devices brought about Phase II. This *Personal Mobility* phase culminated in the successful development and deployment of connected organizers such as the PalmPilot. You can best characterize this phase as enabling synchronization of personal information between the mobile device and a locally connected PC (typically communicating over serial cable or infrared media).

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.