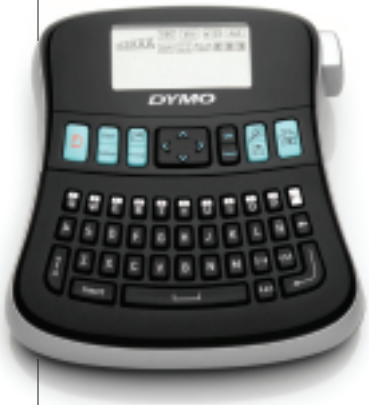
tools of the trade

The **Dymo LabelManager 210D** is a desktop label maker that produces very sharp (180 dpi) one- or two-line self-stick tape labels. You type the label, and the LabelManager centers the text and will remember it in a queue of up to nine different remembered labels. There's a print preview; a choice of lengths; choice of eight type effects, including bold, italic, shadow, and underline; and a convenient cut-off button at the top. Six different character sizes allow for more emphatic or longer labels. Available tapes offer a variety of four colors for text. Tape colors include blue, red, yellow, green, clear, white, or black. When you turn the unit on, the last label is shown in the display. Quick-access buttons permit punctuation, currency symbols, and diacritical markings. There are a total of 132 symbols. You can print up to 10 copies of a label at a setting. The keyboard touch is positive and nicely spaced, and the overall finish isn't something you will want to hide in a drawer. The 210D runs on six AA batteries, and it has an auto power-off to save battery life. www.dymo.com



LabelManager 210D

The **IronKey Secure Flash Drive** from **IronKey, Inc.**, is available in 1, 2, and 4GB versions. All are secured with hardware-based encryption that's already installed. The IronKey Cryptochip provides military-grade encryption that includes a self-destruct sequence. If the chip detects any physical tampering, it will self-destruct. A password manager is included, and you can use passwords with one-click access that bypasses keystroke logging spyware and other attempts to steal your logins. The drive's Secure Session Service has an onboard browser that sets up a secure network connection so you can safely browse from any computer, even across unsecured wireless networks. The metal case is injected with an epoxy compound that makes it waterproof and tamperproof. Along with all the security features, the drive uses SLC NAND Flash in dual channels, which is four to eight times faster than conventional flash drives and much longer lasting. If you're making the IronKey part of your basic plan for portable media (at least two copies in two different places), it's the one you'll probably want to carry around with you because of its speed, encryption,

IronKey Secure Flash Drive

and password and browsing features. www.ironkey.com

Nuance Communications has released the latest version of **PDF Converter Professional 5**, its PDF desktop alternative to Adobe Acrobat. Designed to deliver "Better PDF for Business™," the program was written specifically for government, corporate, and academic organizations. With PDF Converter Professional 5, users can easily convert individual e-mails or archive complete folders of e-mail into PDF format. The converted files will take up half the space of normal e-mail files, and the attachments will remain embedded in their native formats. Converter will let

License Plates and Band-Aids

Michael Castelluccio, Editor

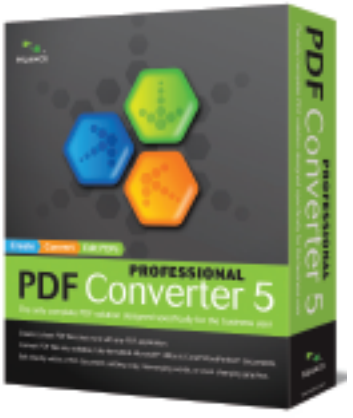
■ WE LIVE IN A SOCIETY that becomes more transparent every day, and technology contributes in a two-fold and considerable way. New devices and databases constantly remove the distance we've placed between ourselves and the official watchers.

A dramatic example of a device that has intruded on our privacy is the security camera. Although a country like England might have wider official networks throughout its cities, the security cam is ubiquitous in the U.S. as well. If you just think about the evening news on television—how often is a story illustrated with murky, distant footage from a remote fixed camera? They are in banks, malls, parking lots, and on utility poles. And whatever footage might be missing from the mounted cameras is often provided in the form of shaky images taken on neighbors' cell phones—cell phones that also create database logs of all your calls and that feature additional transparency with functions like Caller ID.

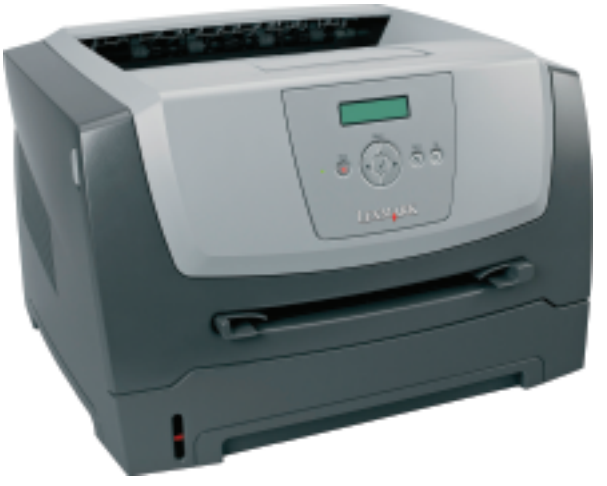
Databases, both public and semi-public, track what you do and who you are. Bank records, dental records, what you last purchased at PETCO, the last book you read—purchased from Amazon or taken out of the local library—there's a paper trail from your daily life that would have staggered the imagination of any medieval chronicler.

continued on next page

you create, print, and edit XPS formats, and you can convert between XPS and PDF documents on the same desktop. You can split larger PDF documents into sets of smaller PDF documents, and you can distribute a PDF for comment and then merge all the sticky-notes and annotations into one master PDF. A compare feature lets you check two versions side by side. The latest version of Converter has sophisticated redaction and document security tools, and it can integrate with leading document management systems used in legal, government, healthcare, and other industries, including Lexis-Nexis, CaseMap, Open Text, and others. www.nuance.com



Does any piece of office equipment take a worse beating during tax season than the laser printer? The **Lexmark E352d** from **Lexmark International, Inc.**, is a solid desktop laser monochrome printer. It features a two-line LCD display and the fastest rated print speed in its class (retails for about $450), delivering up to 35 pages per minute. It also has the highest-yield cartridge option in its class with a 9,000-page aftermarket toner cartridge. It is networked with parallel, USB, and Ethernet connections. Print resolutions include 1200 × 1200 dpi, 2400 or 1200 image quality printing, and 600 × 600 dpi. The printer footprint is somewhat compact at 15.6" × 14.1" × 10.2", yet its capacity is 35,000 pages (maximum usage per month). It weighs 25 pounds. Printing stocks that it can handle include plain paper (16 lb. and 43 lb.), card stock (up to 90 lb.), transparencies, envelopes, and paper labels. Paper sizes range from 3" × 5" to 8.5" × 14". The 250-sheet, letter/legal-size input tray is included, and a 550-sheet tray is available. ■



Lexmark E352 Laser Printer

continued from p. 59

Sometimes a company like Amazon keeps track of what you look at on their site so they can make recommendations about future purchases. Sometimes retail companies lose the records they have, and you and several thousand others are put at risk for identity theft. The watching never ceases, and aggregators like ChoicePoint can produce files that resemble FBI dossiers—even though they offer credit checks, not loyalty and criminal checks. And most of this happens in the background of your life.

Two recent hardware devices illustrate the double-sided nature of technology-induced transparency.

A new license plate recognition system is being tried in Canada and the U.S. The stationary Automatic License Plate Recognition System (ALPR) has been around for a while, but the new mobile version can be mounted on the dash of a patrol car, making it much more effective. A front left-side camera takes pictures of oncoming cars, a front right-side captures cars in the right lane and those parked on the right side of the road, and a rear right-angle camera reads license plates of cars in a parking lot. The system can check up to 3,000 license plates per hour, and it can check for stolen vehicles, outstanding warrants, scofflaws, or the uninsured. When the recorded license plate matches an offender on the database, an audible signal flags the match, and an image of the car comes up on the screen. For about $20,000, it's hard to argue against the benefits of the ALPR.

But what if someone adds a new database to the lists checked by the system? Say someone makes a list of political enemies and asks the local police to be attentive to any possible violations from this select group of licenses. What if an ALPR unit falls into the hands of someone not in law enforcement, someone with other motives and other people to surveil or seek out?

At the February Solid State Circuits Conference in San Francisco, a British start-up, Toumaz Technology, introduced a silicon-backed Band-Aid that will monitor and send to medical centers vital signs for patients who are at home. The chip embedded in the Sensium™ Band-Aid "provides ultra-low-power monitoring of ECG, temperature, blood glucose, and oxygen levels." It sends the information over a wireless network, and it's expected to cost as little as $5 when it's released later this year.

…there's something we can do to make the watchers more accountable.

Toumaz has honed the engineering so the device uses very little power. Its patented AMx™ technology combines low-power radio requirements with smart information handling, producing a disposable monitor that runs on "printed" batteries. The gateway for the transmission of the information can be a PDA, a smart phone, or a specially designed bedside unit.

The Toumaz obviously will be a significant development for patients who want to escape the machinery and confinement of hospitals, but does it also conjure up other uses for the technology—say, clothing labels instead of Band-Aids and maybe global positioning chips instead of glucose measurement devices?

Sure, being connected is a real plus when you can get access files on your desktop PC while you're on the road or when you use a Skype connection so the kids can see you and you can see them during phone calls back home. But what about those networks about which you know nothing that are collecting and sharing information about you? Is tech-enabled transparency erasing your privacy?

More than a few pundits have argued that there isn't anything we can do about the increase of transparency in our culture, especially when often there are such obvious benefits that accompany the liabilities. But there's something we can do to make the watchers more accountable. If the surveillance is an open process, then the watchers will likely be more responsible. If the town is putting up surveillance cameras, ask that their feeds be streamed online on the town website. You'll then know what they are doing. If a credit-reporting agency is required to provide you with a digital copy of the file they are creating about you, you could correct any of their mistakes and maybe prevent abusive intrusions. They probably should also be required to notify you by e-mail when requests are made for your information.

In our legal system, we have the right to face any accuser, so the same should be true of any watcher, and that should also extend to the databases where they keep their version of our profiles. If they're out there looking in through the glass siding on our house or office, shouldn't we be allowed to get a glimpse of who they are? ■