Barcodes & Privacy

Private citizens, especially consumers, have every reason to be vigilant in guarding their personal data. Any and all attempts to collect one's personal data should be challenged. *"Who are you and why do you want to know about me?"* should be questions we all ask all the time. All too often we surrender private information without resistance. More disturbing is when data is collected without our explicit permission.

While others have discussed the protection of citizens' privacy in great detail (see *www.epic.org*), this white paper is limited to the use of barcodes and other auto ID technologies to collect data. This represents Azalea Software's concern about the use of our barcode software and the social implications thereof. Besides, we're private citizens and consumers too.

All too often barcodes and other auto ID technologies like RFID tags are accused of being inherently evil. Please don't shoot the messenger. While barcodes do make data collection faster, cheaper, and more efficient barcode technology shouldn't be blamed for the misuse of collected data. Remember to separate technology from the social context it's used in. Barcodes may be the means to an end but it's the end itself that must be judged.

Like most tools, barcodes in and of themselves are value free. The focus should be on the tool's use. More precisely the person using the tool. A barcode isn't any more "good" or "evil" than a hammer. A hammer can be used to build a school or a gallows. Few of us question using barcodes to track books in a library. Many of us have serious concerns when barcodes used to track citizens' movements or purchases.

Barcodes are innocent and free of original sin. Most are merely lookup numbers into databases. It's those who control the databases you have to be worried about. Privacy concerns should focus on the collection of, access to, and protection of collected data, and any subsequent use or misuse of personal information. If a given company or government agency's practices are suspect or misguided it's not because of a barcode. It's because that group's intentions don't mesh your expectations. Point the finger at the true culprit, the social context the technology is used in. Identify and address your underlying fears and concerns, not the glyph itself.

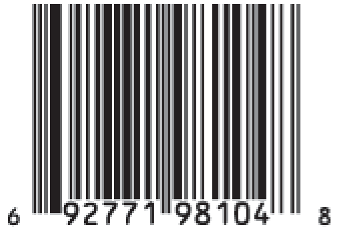
How many ID or membership cards in your wallet or grocery store tags on your keyring? I'll bet most of them have barcodes on them. If you don't trust the issuing company, it's not because they use or don't use barcodes. It's because they're doing something with your personal data you don't like. Barcodes just makes it cheaper for them to do so.

Consumers will voluntarily surrender personal information in exchange for benefits, real or perceived. The prime example is grocery store customer loyalty programs. The stores' pitch is *"If you give me personal data, I'll make special offers to you."* Being suspicious, I signed up for one with bogus personal data until Safeway tied their program to United Airlines. I re-registered using my real identity in order to earn United frequent flyer miles. I the consumer, *voluntarily surrendered personal information in exchange for benefits, real or perceived.* At the time, my concerns about safeguarding my personal data were outweighed by my desire to collect more frequent flyer miles. Draw your own line, draw your own conclusions.

Printing special offers on the back of my cash register receipt based on my spending habits is one thing. Selling my purchasing history to other companies is something else. I assume that Petco knows that I own reptiles and amphibians because I purchase lights, bedding, and live crickets. I signed up for their membership card for discounts assuming that knowledge of my pets isn't an invasion of my privacy.

My concern is the grocery store. Who's to blame when my insurance company raises my premiums or even denies me coverage when they don't approve of my fresh produce to junk food ratio or of my alcohol and tobacco purchases? Should the insurance company be allowed to change my rates based on how I shop? Should they start pitching me new life insurance when they notice that I'm now buying diapers and baby food? Should they deny me insurance when I start buying vitamins for seniors and adult diapers? Or insulin? Either way is the barcode on my customer loyalty card to blame?

No, it's not the barcode's fault. Why? Because I can identify myself to the cashier using my phone number, no barcode involved. Again, remember to separate the data collection methodology from the database's use or misuse.

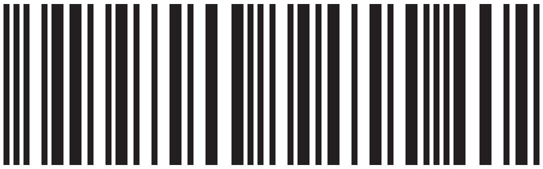


UPC Version A
(retail items in the US & Canada)

Do you want marketers with access to your purchasing history, movie rental patterns, and credit card data to out you, target political candidates to or away from you, or influence your credit check or a job search? Do you get to review the database profile built about you? Do you get to challenge and appeal its contents? Why not? If it's so easy to amass, why isn't it easy to change?

Perhaps worse than building any one database is linking disparate databases together in an attempt to build composite profiles. This is the real power of data mining and the real threat to personal freedom. Beware of those who attempt to own your identity.

In a democracy isn't privacy a guaranteed freedom? Shouldn't anonymity be assumed in a free and open society? The current war on terrorism threatens individual freedom in the name of national security. A clear distinction needs to be made between efforts that really protect us from legitimate threats and those that simply make money for big corporations while earning points for the politicians that propose them.



In today's security conscious world tracking people and things is an international priority. Barcodes and other auto ID technologies provide an audit trail to track terrorists along with ordinary citizens. Where does the line get drawn? Who controls the databases? These discussions need to happen *a priori* with input from citizens, marketers, and those who amass and sell databases. Speak now or forfeit control over knowledge of and access to your intimate details.

And if you want to ignite a real firestorm, consider the implications of a national ID card. If implemented there's bound to be one or more barcodes on it coupled with the potential for abuse. Again, if abuse occurs it isn't because of the barcode.

One concern is that while some barcodes contain a human-readable version above or below it, not all do. This is especially true with newer 2D barcodes like the PDF 417 symbol used on drivers licenses. While some states repeat the information found on the front of the license others use the PDF 417 barcode to store the person's picture or thumbprint. DataMatrix barcodes are finding their way onto bank statements, credit card bills, and even frequent flyer mailings. These small symbols reveal nothing about their contents let alone ultimate use. Consumers have no knowledge of what is being tracked, collected, and stored about them. There is no opt-in option.

Please use this modest treatise as but one source in your self-education about data collection, identification and tracking, and control over details about one's background and behavior. It's your privacy, exercise control over it. Just be sure to asses the risks and dangers with knowledge of the technologies and their application. It's the people behind the tools, not the tools themselves.

And no, barcodes do not contain 666, the mark of the beast.

Revelation 13:16-18

azalea
software, inc.

www.azalea.com

Barcode nerds since 1992.
And damn proud of it.