

Inside 1to1 Privacy

Date: 04/11/2007

Issue: April 12, 2007

People: Jay Cline

Comparing Coffee Shop Privacy

The next time you take a call from a consultant who sounds like he's in a noisy Indian call center, ask him what coffee shop he's in. Chances are, he's perched in one of the variety of cafés launching wireless hot spots and changing the way America does business. This new trend also is adding an intriguing new dimension to corporate information risk.

Have you noticed how quickly the laptops have sprung up on the tables at your favorite Starbucks? Or eavesdropped on the increasing number of teleconferences being conducted on the sofas around the Caribou fireplaces? By expanding wireless Internet access this past year, these coffee barons have tapped into a huge daytime market of mobile professionals.

But this new business model presents some nagging questions for consumers and privacy professionals. Which coffee chain has the most secure WiFi? Which coffee shops are best configured for private conversations? Which brand does the best job respecting customer privacy online and through its loyalty card?

Before spilling the beans, a little about the coffee-shop landscape in America. It's dominated by Seattle-based Starbucks, with its 12,000 stores and plans to expand to 40,000 around the world. Think of the coffee king as a massive, \$8 billion distribution network for not only coffee, but music, books, magazines and anything else you do when you hang out and unwind.

Starbucks' distant rival, Minneapolis-based Caribou, counts 464 stores in 18 states, and is also riding the coffee wave of rapid store expansion.

Other players topping the U.S. list include: (3) Tim Horton's (subsidiary of Wendy's International, with 336 stores in six states and 2,700 in Canada), (4) The Coffee Bean & Tea Leaf (HQ: Los Angeles, with 265 stores in Western states and 256 more in Asia), (5) Seattle's Best Coffee (a Starbucks subsidiary with 160 stores), (6) The Coffee Beanery (HQ: Flushing, MI, with 135 stores in the U.S. and 25 overseas), (7) Peet's Coffee & Tea (HQ: San Francisco, with 112 stores), (8) Dunn Bros Coffee (HQ: Minneapolis, with 80 stores), (9) Tully's Coffee (HQ: Seattle, with 79 stores in five Western states, and 321 in

Japan), and (10) Port City Java (HQ: Wilmington, NC, with 55 stores in 10 Eastern states).

So when consultants are emailing confidential documents from the coffee shop, how safe are they? It depends.

At Starbucks, wireless is offered through T-Mobile accounts that cost \$20 per month and require users to authenticate through T-Mobile. Caribou offers free wireless access through Wandering WiFi. The Coffee Bean offers AT&T accounts that cost \$20 per month for non-AT&T customers. All of them use unencrypted connections, so anything sent through unencrypted email systems such as Yahoo! could be "sniffed" by someone with the right tools sitting in the coffee shop. If a company's consultants use these WiFi networks to log in through the corporate Virtual Private Network (VPN), though, their communications will be safe.

And what about those private conversations? Nearly all the seats in these coffee chains are out in the open, adjacent to other seats, making it fairly easy to listen in on business.

And the coffee cards – was there a clear privacy leader? An online purchase of cards from every brand revealed that just four of the top 10 – Starbucks, Caribou, Coffee Bean & Tea Leaf and Peet's – offered promises not to email customers or share their information with other companies without their opt-in consent.

According to Terry Mansky, Vice President and General Counsel at the Coffee Bean, his company also provides customers a privacy pamphlet encouraging them to enable their personal firewalls, disallow file sharing on their PCs and create a VPN connection.

But here's the disappointing note: only one – Tim Horton's – advertised it had a Chief Privacy Officer; none had earned a TRUSTe or BBBOnline privacy seal; and one – Port City Java – didn't even have an online privacy policy.

So what does this all mean for corporate privacy agendas in 2007? Nothing major. But it couldn't hurt to send a reminder to employees not to email Confidential or Privacy Restricted files from the WiFi networks at coffee shops, libraries or hotels unless they're on the VPN – and to find private places for their business conversations.

Cline is President of Minnesota Privacy Consultants. He can be reached at cline@minnesotaprivacy.com.