



Using research to determine product attributes and stratification for the design and marketing of user authentication.

[Study 2:
**An Ethnography of airport
travelers regarding data safety**]

By Mark Schraad

April 24, 2006

Study 2: **An Ethnography of airport travelers regarding data safety**

In the 1990's the World Wide Web was gaining momentum and online commerce was becoming one of the most dramatic economic forces in the civilized world. People were drawn to the savings of online shopping and the convenience of UPS front door delivery. Meanwhile, a mild hysteria was growing among those less familiar with computers and the digital world. Their fear was that transmitting a digital version of a credit card number was more problematic than the recital of that same number over an analog phone line to Sears & Roebuck. Parents became increasingly aware of how easy it was for predators to pry household secrets from children inside of online chat rooms.

Studies funded by the Annenberg Foundation revealed that parents were at least as worried about the leakage of financial and health information as they were about their children's exposure to pornography and predators (Turow & Kavanaugh. 2003).

In 2002 Sync Magazine reported that nearly 12,000 laptops were left in taxicabs over a six-month period. Another report cites 20 laptops a week being turned in at the Los Angeles International airport as lost or stolen (Sync, 2002).

During the first months of 2005, newspapers reported almost daily about the rash of stolen laptops from the likes of the California Democratic headquarters, major universities, financial organizations, and even ChoicePoint, a leading provider of background and credit checks. It is hard to read a news report without hearing of yet another identity theft. By the end of 2004 one in six Americans had become a victim of identity theft.

More and more Americans are making use of "one click" shopping. The convenience of online purchases without the hassle of typing in a credit card number matches today's hectic lifestyle perfectly. Paying bills and managing bank accounts online with Quicken and other products is a convenience most of us can appreciate. But there is a downside. Digital storage makes for quick and nearly flawless duplication. The fears of those early techno-phobes are being realized. But the theft is not occurring during transactions, rather it is occurring as a result of the information's storage. The lack of effective security is indeed betraying those using the digital world to execute financial transactions. Was the technology to blame? Was it carelessness, human error, or was it poor behavioral engineering?

Research reveals that a very small but growing proportion of identity theft occurs as the result of digital information. Most identity theft occurs using stolen credit cards, invoices, access to personal information numbers (PIN), and passwords. Most of that information is found in residential

trash. But the ease with which digital information can be duplicated and transmitted makes it an ideal method for efficient theft.

Americans are increasingly using their computer as a digital wallet. A wallet that can easily be connected to the world through the Internet. More than 50% of American households now have broadband Internet access.

In April of this year the problem had become so commonplace that Satirist Andy Borowitz (Borowitz, 2005) wrote about a fictional identity thief who has stolen over a half million identities in just a couple of years. He reportedly gave all but four back, declaring them "worthless." After spending months to steal identities from a financial institution hoping to reap millions, he said they were "little more than a garbage dump of unpaid student loans and overdue Blockbuster bills."

"Everybody's running around worried about identity theft these days." "All I can say is, don't flatter yourself by thinking you have an identity worth my time."

He even suggested that institutions be forced to flag worthless identities, enabling hackers to focus their energies elsewhere.

Interested in the sort of concerns Americans have for the safety of their identity, I wondered what, if anything, they were willing and able to do about it. To find out I was going to have to be where people were using their computers. I would need to watch them and talk to them. I would need to find people that were using their computers for financial transactions. People who use their computers as an organizational tool and keep it with them most of the time. This led me to business people who were traveling with their computers. I suspected that those computers had become central to all things organizational and financial. I was planning to live among the "road warriors."

In the spring of 2005, I spent a considerable amount of my time in airports. I traveled for business, for school, and for pleasure. I was in fact a part of that community that organized its work, play, and financial transaction on a laptop. I also went to airports to watch and learn. I sat in airports for hours with no place to go. I sat in bars and in coffee houses. I sat in lobbies with my laptop and an old boarding pass to look like I was traveling. I observed and tracked behaviors, frequencies, and counted populations. I watched people at airports waiting on departure flights and I observed people arriving on planes about to gather their luggage. And I watched people wrestle with their luggage as they negotiated taxicabs, buses and automobiles, many with laptops in tow.

Methodology

To learn more about the lifestyle and concerns of the laptop traveler or 'road warrior' it is necessary to live in their space. Travelers are likely to frequent airports, taxicabs, rental cars, trains, restaurants, and hotel rooms as well. Hotel life is a place for the frequent traveler to find quiet and solitude and was too intimate for this study. I was not looking for insight into the individuals so much

as the collective. Finding travelers in cabs, trains, rental cars, or restaurants would require a considerable amount of time with little efficiency. My work in the field would be short and precious so, to make the most of it, I decided to concentrate my efforts in airports.

Traveling on commercial airplanes requires some waiting time. The traveler must be in the airport for security and scheduling, yet it is time with little to do. The efficient traveler will use this period for small tasks that can be done relatively quickly and that are not urgent. The airport would combine a dense population and an optimal opportunity for observation.

When I was in the field, I would put myself in the role of a traveler. This served two purposes. I am a member of this population, but rarely did I think of my own experiences in the context of this study until it began. Researcher introspection allowed me to live the life - to be closer to and part of the experience. It also allowed me to move fluidly among the others. I was not an outsider, but one of them. In my initial visits to the airport I was actually scheduled for departure flights. Some go early, get oriented and then have plenty of time for observation and hopefully conversation. For my later visits I would be in the airport specifically for fieldwork without a travel agenda. Each time I spent the better part of a day there, usually with my laptop and my carry on backpack in tow. I felt it important to be part of the environment and to look the part of a fellow traveler even when I was not traveling. I even went so far as to carry an old boarding pass envelope with me. I wanted to appear as much a part of the environment as was possible.

My intent was to experience this environment on three levels. First, I wanted to observe what most of us probably do not take time to see. Arriving at the airport for a flight even if you fly frequently can be stressful. Flights are relatively expensive and they typically leave on time. If you are late it is unlikely that the flight will wait, so getting there on time is important. Airports are large and typically have multiple airlines with many flights leaving and arriving. Finding the right gate is another concern. The focus on security has, of late, added another source of stress and time. Airlines now recommend that passengers arrive 90 minutes prior to take off – more for an international flight. The logistics of these security measures complicate the use of this time, as detailed elsewhere in this study. For these reasons, most people don't take the time to look around. Travelers are focused on the essential details required for making sure to get on the plane and that it is the right plane. I wanted time to look at what goes mostly unseen. I wanted to take in and record the environment, the behaviors, and the subtleties that are most likely missed by the average traveler.

The second experience I was looking for was that of the travelers themselves. I intended to make multiple business trips over the course of three months. During those trips I would be bringing my laptop computer in my backpack. I would make a point to use it in the airport, check through

security with it, and even try to use it on the flight. I wanted to understand through researcher introspection what it felt like to operate and deal with computer use on the road.

Lastly, I wanted to hear about the experiences, concerns and issues of others regarding life on the road with a computer. What were the problems, what were the efficiencies, and how did others cope with them? That would require finding a way to strike up conversations with other road warriors, without alarming them or seeming an outsider. To accomplish this, I was frequently parked in the airport with my laptop plugged in and running. Other times I would find a seat near someone that was using a computer and go through the process of setting up, turning the unit on, and logging on to the local wireless network. This process can be problematic and it turned out to be an excellent way to start a conversation. Asking the person across the aisle if they were getting a strong signal told me to some extent what they might be doing, if they were online, and it gave me some indication of their technical savvy. Most people I encountered were very willing to help out by providing some insight.

Once I had talked to them and developed some rapport, no matter how small, it was much easier to continue the conversation. Often times I would ask for some advice from the savvy traveler. I would then explain to them the nature of my research and ask for their contribution and insight. I was never turned down when I used this approach.

My conversations were always open ended. When the respondent wanted to take the conversation, in a different direction I would let them. In cases where it was up to me to continue the conversation I had a list of questions to draw from. I would inquire as to how often they traveled, was it usually for business, and did they usually carry their laptop. I typically asked if they carried on or checked the computer, how they kept it safe, and what, if any, were their concerns regarding the loss of their computer.

While this methodology is solid, the results may be somewhat limited in accuracy. To some extent quantity is important. I visited 4 different airports on 8 occasions. During two visits, I had a total of four very insightful interviews. This is a far cry from a reliable sampling. Further, most of my fieldwork took place in Kansas City International airport. This is not a major business market, nor is it a major hub for any airline. I would guess that the majority of people I witnessed were Midwesterners. From this study it is impossible to determine if there is a southern, east coast, or international shift in these attitudes. Additionally, these observations of behavior were fairly short in duration. Further studies in other airports may reveal different behaviors. Interviews are a form of voluntary disclosure. I know and understand what these individuals said, but that does not always be consistent with their behaviors. That they expressed a particular concern or opinion does not mean that they would actually act.

Theories prior to fieldwork

Early in the conception of this study, I spent some time thinking about the nature of laptops and the implications of a lost or stolen computer. I theorized about the concerns for that loss. I determined that there were three primary levels of concern. The first is for the loss of the computer hardware. Laptops are expensive, often to the tune of thousand of dollars. But nearly all owners have insurance polices, and certainly all businesses carry insurance. The laptop would almost always be replaced at minimal cost to the user. The second level would be for loss of data and the time required to reinstalling software. Most companies and proactive individuals would have a back up system. While inconvenient, the configurations could be restored. The third level of loss was that of the information on the computer. What if it fell into the wrong hands? Recent cases of industrial espionage and identity theft would leave one to believe this was the largest of concerns. Most credit card companies claim at least a portion of this potential liability. But I was curious, was the typical laptop traveler concerned or even aware of this last issue?

Observations in the field

I spent a considerable amount of time in the field observing traveler behavior. At times I counted the number of travelers in sight, the number of carry-on bags that could contain laptops, and the number of laptops in use. In all of my counting, it seemed the majority of computer users were male. Most of them appeared to be traveling for business, either alone or with one other person. Dress was used to indicate if the travel was there for business or leisure. There is potential for error in this assumption, as it is not uncommon for leisure travelers to be in dress casual attire. It is also possible for professionals to dress very casually.

Laptops are sometimes equally difficult to identify. The simplest of course is the laptop in use. Often there is a designated bag, sometimes with the manufacturers logo. Those are the easy ones. But many carry-on bags and briefcases are now indistinguishable from laptop bags. Further, many travelers use backpacks. Many of those come with laptop specific storage compartments that are difficult to detect.

In all twelve observations I never saw a traveler leave a laptop completely unattended. On several occasions I did witness people asking someone to watch their bag, but never an open laptop. In two cases they did not appear to know the person. In each of the other four cases the two appeared to be traveling together. I witnessed many situations where an individual packed up their laptop and carted it to the bathroom, the newsstand, or for a cup of coffee, only to bring it back to the same seat and unpack it again.

One of the more interesting observations was of the value of battery life and a good supply of power. Laptop users (as well as the occasional mobile phone user) tended to gather around power

outlets like cities on the river. They would often negotiate or take turns occupying the two or four plugs available. I observed on several occasions travelers walking through seating areas looking along the wall for an outlet. Power outlets were more common in the bars, coffee shops, and restaurants than in the common seating areas.

When I talked with a traveler named Kent at Kansas City International Airport (KCI), he mentioned that he works on his computer while waiting for a flight on about 25% of his trips. It is rare for him to be out in the public area. He flies regularly on Delta, and it has a Captain's Lounge, a semi-private place for frequent fliers that has free Internet connection and plenty of plug-ins plus, "more comfortable seats and free coffee." His Southwest flight was unusual, and he did not seem particularly pleased about it.

Another observation was the pairing of a laptop with a mobile phone for conversations. This was so prevalent that in one single session of over four hours, I was unable to locate a single laptop user who was not also talking on a cell phone.

Revealing conversations

In nearly all airports there are one or more sources of wireless Internet access. I found that one of the easiest ways to start a conversation was to ask the person "what kind of signal they were getting." Laptop users are keenly aware of the problems associated with wireless networks. These networks broadcast in relatively small zones and metal windows or mirrors disrupt transmission. Most laptop users are sympathetic and willing to help out with a second opinion or some configuration advice. In many cases this was my segue to more important questions.

Traveler concerns

My first question was whether they were here on business or for leisure. I never found a leisure traveler using a laptop with which to have a conversation. My second question was whether they ever checked their laptop as baggage. No one I spoke to did. I asked why and began to get to some of the concerns travelers have for the safety of their computers. The general issue was their perception of how luggage is handled and that the laptops were fragile. They wanted to make sure that it would be safe from harm. Further, the advice given about carry-on bags was to keep it with you at all times and not let a stranger have control. This seemed appropriate for care of any valuables. Most of the travelers I observed and spoke with made a point to keep everything with them or at least within sight for the entire journey.

In nearly all cases the primary consideration was that they would have the laptop in working order for an impending presentation or meeting. When I mentioned the expense of the loss of a computer, I nearly always got a response about insurance. Often that response was like Chet's, "it's my company's, I am sure they have it insured." Computers get faster and cheaper every day.

Kent mentioned while we talked, "I've been using this one for a couple of years, it's probably not worth anything."

I met Dave that same day. He is a sales manager and flies primarily for business. Dave is in his early forties and lives in Minnesota. He supervises a group of 30 sales reps with territories around the country. All of his "guys" travel with laptops. A lot of them use laptops while on the plane, but many had stopped because seating is cramped and the laptop was difficult to work with in such a small space. To help with this, Dave's company has issued Blackberries to all of its reps. A Blackberry is a mobile phone with contact, calendar, and e-mail applications. This allows users to accomplish most of the laptop's functionality without the laptop. Dave also said he had moved customer data to a Web-based service, so the information is centralized and not stored on the laptops. "There is still a lot of company files – PowerPoints and other stuff on those computers," but he is now a lot less concerned. When I asked about company credit cards and his rep's personal financial information, he did not seem concerned at all. He said, "I don't lock up my wallet. I guess I keep track of my laptop and cell phone the same way." While this seemed mildly contradictory he seemed pretty confident in his reasoning. Dave said that he does not use a password on his computer, explaining "its just a hassle."

As I was about to pack my things and head home, another traveler sat down just two seats away. He said hello as he unpacked and I decided I had time for one more conversation. His name was Mike, and it was apparently very important for him to check his e-mail before his flight. I asked him a few questions and got fairly standard answers until I got to the topic of the safety of his laptop. He said he had a startling realization recently as a result of loosing his. He realized he needed to think about the value of his data – backing it up and securing it. "Just last week, I got home from a trip and realized I did not have my laptop, and I panicked. I called the airport and they had found it, they said they would have it in the security office waiting for me so I headed right back. When I got to the office, there was no one around. But my laptop was sitting on the chair with no one around. I was in a hurry, so I just grabbed it and headed home." Mike said the data on his computer were new – stuff from a client that he needed to work on right away. It would cost him time and reputation with such an embarrassing loss of confidential information.

Was I one of them? Self study?

During the initial portion of this research, I realized that I was in fact a part of my target population. Because of my rather nomadic lifestyle, I had centralized my work, research, studies, personal communications, and finances on my laptop. This centralization and mobility allowed me a considerable amount of freedom. With wireless technology, I could setup at nearly any coffee shop or public place, check and send Emails, work on any number of projects, and generally make very

efficient use of my time. I had several trips planned – some 15 flights over a ninety day period – so I took the time to note some of the issues that affected me while traveling with a laptop.

Things have changed radically for air travelers since the 9/11 tragedies. Airport security is at a feverish pitch and traveling has become a huge inconvenience. The layout of the airport had changed. In most airports, there was a common section of the airport that nearly anyone could travel. The gates themselves were in a separate area. In every airport I visited, the security station separated the common section and the boarding area. Lines formed to get in to the secure gate area. Often the lines were very long. Once in the secured gate area, if you came out, you would need to go back through security. At the security station, travelers are required to remove jackets, the contents of their pockets, belts, and shoes. All laptops must be taken out of their bags and checked separately. All bags were x-rayed. At random, some travelers are singled out for a more in-depth check. They were waved with a metal detector wand and often their luggage was searched by hand. This process took considerably longer. Once through the process travelers are left to hurriedly dress and repack their bags. The process is unsettling and invasive.

Twice on one trip and once again on another trip my laptop was hand inspected. The opened it up and turned it on. They swabbed it with cotton and then fed that cotton into a machine that checked for explosives. I wondered, "do people use laptops to make bombs?" Making an exception to my usual curiosity, I elected not to ask.

Most of my research took place at KCI. This airport is organized into three terminals, A, B, and C, each a large circular ring with car parking on the inside and planes parked on the outside. The main corridor runs in a large arch. The gates are located along that arch on the outside. This apparently posed a logistical problem for airport security. They solved it by building glass walls between the gate areas and the common hallway. Gates were walled off in groups of three and four to a section. There were no bathrooms, no restaurants, and no newsstand within the secured gate areas at KCI. This posed a logistical problem for me. I was supposed to get there early and check in for my flight. But then once I passed through the lengthy security check, I would no longer have access to food, drink or bathrooms. With a 45 to 90 minute wait, that could be a long time. If I got a newspaper, a cup of coffee, a bagel, that was a lot of extra stuff to get through security. I was already carrying my laptop, my bag, my ticket and identification, my jacket and all of the contents of my pockets... oh and my belt. Could they have made this any more difficult?

My choice was to stay outside of the secured area for as long as possible. So in most of my trips to KCI, I found a seating area to camp out in prior to entering security. The downside was that when I did go in there was a longer line.

In each and every airport I experienced, there was a regular and frequent announcement about keeping track of my bags, and not letting anyone tamper with them or give me anything to put in them. In keeping with this warning, my laptop never left my side. I knew where it was the entire time.

I was most likely to use my computer during layovers. Particularly if I was changing planes and had more than 30-40 minutes. I would open the computer, turn it on and check Email. Rarely would I actually work on projects unless I was approaching a deadline. I also used my computer prior to departures. That was especially true if I was boarding for a long flight. I have never used it upon arrival. There is plenty of motivation to get out of the airport and away from the plane.

Rarely did I find it convenient to work on the computer while in flight. Logistically, with people getting up, drinks and snacks being served, and considering the small space and lack of connectivity to the Internet, it just wasn't worth it. During most of my flights I did not have access to power, so I would have had to use up precious battery life during the flight. Sure, traveling with a laptop was a bit inconvenient. But I would carry a bag onto the plane anyway. And the level of additional hassle was minimal in comparison to traveling as a whole. The benefit of having a centralized source of work, play, communications and study enable me to make better use of my time. And time is an exceptionally valuable commodity.

Conclusions

For most of the people I talked with the primary concern regarding the safety of their laptops and data was short term. They specifically needed it on this trip, typically for a meeting they were headed to. The long-term and the financial risks, no matter how real, was of less concern. Nearly every person I talked with recognized that there was a financial liability but with the exception of Mike, there was little motivation to do anything about it. In two of my interviews, I asked what it would be worth to have your data completely locked up so that if someone got to their computer they could not access the data. Was a hundred dollars too much, maybe two hundred? Both seemed to think that the money was a reasonable expense, yet neither seemed ready to act on the problem. I likened it to so many issues that we just don't bother to deal with.

We have known for years that with some regular exercise and slight changes in diet, Americans could extend their lives and delay the onset of cancer, heart disease, lower health care costs, and reduce hospital stays. Yet, those behaviors are not easily changed. Change is hard. And given the choice of "change or die" many still can't or won't change. The fast food industry has never been stronger and Americans have never been less healthy.

I am pretty sure that for the majority of people, asking them to change their behavior to safeguard their identity and their finances is a tall order. Ultimately, the responsibility will have to lie

with employers, credit card companies, banks and maybe even computer manufacturers to deal with the loss and prevention. Certainly some computer users will take measures into their own hands, but it will likely be a small number. I wonder if it will be a greater percentage than those who get regular exercise and avoid processed foods?

This is a component of research done in part as a thesis project in graduate school and initiated during my role as Vice President of Marketing. It is highly topical to Griffin Technologies without which this project would not have been necessary or possible. My thanks to all of those individuals for their help and support.

Tables, figures and some of the conclusionary content have been omitted from the versions published on the web site. Some of that content is available by request.

For further information please contact me at mschraad@markschraad.com.