Privacy, Security and Fraud: Is there a balancing point?

As seen in Payments Business Magazine (www.paymentsbusiness.com)

Do you ever wonder how you can possibly keep ahead of these, given how quickly technology evolves? Remember when mobile phones first introduced cameras? Most of were thrilled with the new functionality. It didn’t take long before bad people started to misuse the cameras, often to violate people’s privacy. Technology being abused and misused is a cycle that we see all too often.

Is there any hope? Yes, there is!

Where to Start

On the privacy side, we have two laws in Canada; PIPEDA the Personal Information Protection and Electronic Documents Act (PIPEDA) which is Canada’s private sector privacy law and The Privacy Act which covers the personal information-handling practices of the federal government. The Office of the Privacy Commissioner has a great deal of helpful information at http://www.priv.gc.ca. Check it out for information that can help you both professionally and personally. Ontario also has a Personal Health Information Protection Act. Now, if the thought of having to read through a legislative Act strikes fear in your heart, you’ll be glad to know that Fair Information Practices are the underlying premise of these ACTs and they are common sense principles.

Privacy Policy Plus

Many of us have privacy policies that have morphed over the years as we introduce new products, services or technologies. The bolt on approach can sometimes work, but you need to step back periodically and review your overall privacy position. Question whether your goal is simply to be compliant with the law. Do you want to make privacy a marketing and competitive advantage? Do you want your customers to see you as a trusted entity? The answers, of course, will be dictated by what you sell and how privacy sensitive your customers are. Once you’ve decided on your strategy, it’s time to take a holistic look at your policies. Here are some of the things you should consider.

1. Are your policies consistent across your organization? If one area of your company states that it does not collect specific personal information, but another part of your company does, you’ll need to make that clear to your customers or people who visit your web site.
2. If you tell people that they can control privacy settings, make it easy for them to do it.
3. Understand the risks of using the term “We may...” in your privacy policy. It doesn’t engender trust in the reader.
4. Think about stating your policy in terms of the fair information practices (see https://www.priv.gc.ca/leg_c/p_principle_e.asp for the list)

5. Do a Privacy Impact Assessment. There are many in the market, as well as competent consultants. You want to look for a PIA that deals with the personal information from the time you first collect it until you securely dispose of it. You’ll need to think about everyone that has access to the data throughout that period. Determine what they can do with the information. That is more than whether they can view, add, change or delete information, but whether they can print, copy, transmit or otherwise affect it.

ACT Canada and the Office of the Information and Privacy Commissioner Ontario have developed several of these procedures to deal with chip card applications.

6. Make this personal. Think about your mother. What privacy protection would you want her to have?

Face-Not-Present

Are you tired of having to provide a lot of personal information every time you access specific web sites? We all understand that certain sites need to be absolutely sure who we are before granting access to assets such as bank accounts or health information. Nonetheless, over the years I’ve come to the conclusion that we make things more complicated than necessary.

I am me, not me the driver, me the patient, me the traveller or countless other “me’s”. I have the right to drive because I have passed the required test and have not broken the driving rules that would cause me to lose that right. My rights and privileges will change, but I will always be me. In a “face-not-present” world, why can’t I have a “me” certificate that assures the other end of the web portal that I am who I say I am. The fewer times I have to provide my personal information, the better I feel about my privacy.

New and Neat: Thinking Like a Consumer

If you are using a web site to provide services, the state-of-the-art is to not ask me or your other clients to provide more personal information, but to use something we already have and that you trust. For example, several Government of Canada web services may now be accessed by using bank credentials. Neat – it’s something I already have and I know how to use. This is a great example of going one better than thinking outside the box – the government of Canada and SecureKey, who make this possible, have expanded the box!

For the government, it was important to get citizens to use the cost effective web portal but some people found it difficult to remember their sign-on details and some were concerned about privacy. By thinking about it from the consumer’s point of view, the government solved the problem.
So... the Balancing Point

If you approach things from a privacy perspective, you will design systems that have tight security. The first time we used the Privacy Impact Assessment Procedure for Smart Cards, the application developer was surprised that we ended up with a 110 page report when we had expected 20. They were happy that we had also found all the security gaps in the process and delighted that they could use privacy as a marketing tool. You really can balance privacy and security for the benefit of your clients and to the detriment of the bad guys.

Catherine Johnston, President and CEO, ACT Canada

ACT Canada
Insights • Networking • Visibility

Since 1989, ACT Canada has been internationally recognized as the stakeholder association that drives payment evolution and digital identity. Stakeholder dialogue drives profitable decisions. Join us.

For information, please visit www.actcda.com.