The Privacy Policy Problem (4):
Reality Hits Home

by M. E. Kabay, PhD, CISSP-ISSMP
CTO, School of Graduate Studies
Norwich University, Northfield VT

In the last three columns, I’ve been looking at the complexities of protecting client or prospect privacy (personally identifiable information or PII) in an interconnected world.

The problem is greatly complicated by the web of relationships that can develop in the world of marketing. The relationships can involve remote firms that have contracts with your marketing division or contracts with firms that are one or more levels removed from direct interaction with your organization. Worse still, some sites may even be run by rogue organizations which have never had any contractual links whatever with you or with any of your legitimate agents. These facts make it almost impossible to prevent PII from visitors interested in your products, services or programs from being spread to other institutions.

You are left with a distasteful duty to warn all applicants that you can control the use of their PII only when they enter data into forms directly under the control of your own staff or of firms which have contractual obligations to follow your privacy policy. Examine your privacy policies to see if you should include explicit warnings that they apply only to your clients and not to people asking for information. It may make sense also to include a warning about the impossibility of your controlling privacy policies on Web sites outside your own domain.

In terms of response to complaints, you will have to continue being prepared to respond, basically, “Caveat emptor” (buyer beware). You can prepare general texts regretting (and repudiating) the impression that your organization has violated any privacy policy and explaining that anyone entering data on _any_ Web site would do well to examine the local privacy policy for clarification of what degree of protection is offered for PII. If the privacy terms seem too loose, privacy-conscious individuals may decide to skip using those Web sites; instead, they can look for safer, more trustworthy alternatives that provide the same access to the desired information.

As mentioned above, an additional and probably intractable problem is that not everyone who uses your name and your logo necessarily has any business relationship with your organization at all. Phishing (using fake e-mail that looks like legitimate messages from well-known organizations) and pharming (using fake Web pages that look like legitimate Web sites belonging to well-known organizations), for example, are based on impersonation of business entities. Someone could easily use your organization’s name and logo on a form claiming to be related to providing information about your organization, products, services or programs – and then simply use the collected PII for their own purposes. Failure to send the victim the requested information reflects badly on your perfectly innocent and unknowing organization; selling the PII to spammers makes you look terrible. And what are you going to do about it?

If someone is abusing your trademark or your servicemark, you can sue them for misappropriation – if you can find them. With fraudulent Web sites appearing and disappearing with lifetimes measured in hours or days, it is going to be hard to locate the criminals who are
ruining your reputation. Going after the service providers is going to be tough because many jurisdictions have laws protecting Internet Service Providers, including some Web hosting services, from legal liability if they pay no attention to the content of what their clients are putting on the Web. From a practical perspective, what can a CISO do to stop this kind of abuse?

In practice, your organization can hope to obtain redress only from responsible, stable firms with which you have signed contracts. Such firms will care about their own reputation as well as yours and will respond to both notification of abuse and the possibility of legal pressure. Criminals, however, are out of your control, especially if there are international boundaries in the way. The chances of getting any response, let alone cooperation, from law enforcement agencies in many parts of the world where criminals abuse the Internet are virtually nil.

Readers concerned with measuring the extent of the PII-violation problem for their corporate identity may want to institute a systematic program of regularly scanning the Web using search engines. In addition, you can test third-party sites that mention your corporate name or claim to be offering managed marketing information by using a list of fake unique identifiers (M. F. Kabay, M. Q. Kabaye, N. B. Kabbay . . . ) and their corresponding one-time use e-mail addresses (mfkabay@<$string1>.com, mqkabaye@<$string1>.com, nbkabbay@<$string1>.com . . . ). The unique identifiers can be assigned to the specific Web pages under test and recorded in a list, a spreadsheet, or a database for later reference. Any e-mail to a test address originating from an organization other than the managers of the place where the unique identifier was originally used indicates potential abuse or violation of contracts. Similarly, filling out a form that claims to be sending people information about your organization but finding that you never receive a response tells you that there’s something fishy about the site. If there are many test names and one-time e-mail addresses, you can consolidate the traffic for the compliance officer by having all e-mail that is sent to the test addresses auto-forwarded to a single mailbox for easier analysis.

It’s not going to be easy, but at least you can put your privacy-protection measures in place before you face a major PII disaster. Keep your eyes open, follow up on abuse of your corporate identity, and make your own policies clear and effective.

I wish I had something better to offer, but that’s about it for now.

* * *

M. E. Kabay, PhD, CISSP-ISSMP is Program Director of the Master of Science in Information Assurance <http://www.graduate.norwich.edu/infoassurance/> and CTO of the School of Graduate Studies at Norwich University in Northfield, VT. Mich can be reached by e-mail at <mailto:mekabay@gmail.com>; Web site at <http://www.mekabay.com/index.htm>.

Copyright © 2008 M. E. Kabay. All rights reserved.

Permission is hereby granted to Network World to distribute this article at will, to post it without limit on any Web site, and to republish it in any way they see fit.