The Privacy Policy Problem (1):
A Model Policy

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

Many organizations strive to protect the confidentiality of prospects and clients. In this column and the next three, I want to explore issues relating to privacy policies and the sometimes problematic relations between legitimate, well-meaning institutions and the commercial organizations with which they do business – and the criminal organizations which abuse their good names and reputations.

Norwich University’s Privacy Policy< http://www.graduate.norwich.edu/privacy_policy.php > stands as an excellent example of a clear, well-written and comprehensive document – an example that could usefully be considered by readers of this column who may need a sample policy for their own organization’s use. Links to the policy are available where visitors may enter personally identifiable information (PII); for example, the admissions-related pages have links at the bottom of every page with a data-entry form. Specifically, the policy makes the following essential points (quoting with added commentary in square brackets):

- “Norwich University requests a certain amount of information from our clients in order to provide the online experience.” [A privacy policy should begin with a statement of the purpose of data collection.]
- “Although we gather names, e-mail addresses, locations and other personal information (dependent on the platform being used), all information is kept confidential.” [The introduction makes the intent of the policy clear.]
- “Information is used for course registration, billing purposes, providing knowledge about our client base, managing our services and to assist us in making the online experience the best possible.” [These are useful clarifications of the intended applications for the collected data.]
- “Information about who may login in from time to time is analyzed in order to allow us to monitor and maintain our network. Information about our clients may also be used to provide feedback to our institutional clients; at no time do we share this information with an outside source. We may, from time to time, examine a platform for statistical purposes, but we will not identify any individual in doing so.” [These are specific constraints on how the data are to be used.]
- “Information placed on our systems may be available to others on our various platforms, depending on the platform chosen. This information is used strictly to allow a client to participate in their individual course(s) and is kept confidential. We will not divulge private information to any unauthorized person.” [These sentences add some more well-defined constraints.]
- “It is understood that information entered on our system(s) may be seen by a variety of people administering, participating in or monitoring any part of the chosen platform, within the reasonable guidelines set therein.” [Although this alert may seem obvious to information technology specialists, it is worth reminding non-technical people of the reality of data collection.]
- “[Norwich] will also comply with any legal request(s) made by any body so authorized for information, should proper documentation be provided to us.” [This is the get-out-of-jail card that puts users on notice that the University will fully comply with all
appropriate court orders and other legal obligations from duly constituted authorities.

In my next column, I’ll look at the problems which can occur when working with independent partner organizations that may have different privacy policies from one’s own.

* * *

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://www2.norwich.edu/mkabay/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.
The Privacy Policy Problem (2): Controlling Business Partners

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

In this series of four articles, I’m exploring privacy policies. Today I’ll continue with an analysis of potential problems due to independent partner organizations working on behalf of their clients without adequate supervision and coordination.

First of all, if one of the sites which you are paying is selling or otherwise sharing the names and contact information of people who enquire specifically about your products, programs, and services to your competitors, you may want to discuss their practices with them. On economic grounds alone, such behavior may be counterproductive; worse, it may tarnish your reputation as an institution of integrity or erroneously give prospects and clients the impression of improper behavior. Therefore, your organization should periodically audit sites marketing information about you on the Web.

For example, in researching this question I found sites whose privacy policies do little to protect visitors’ privacy. For example, some of these policies state that information collected on the site may be shared with business partners, service providers, sweepstakes and promotions organizers, subsidiaries, law enforcement, and non-affiliated companies.

One text about non-affiliated companies would raise concerns for anyone. The policy begins reassuringly, “We do not share Information with any non-affiliated third party except: (1) in select circumstances when Our business partner refers you to Us and you give Us permission to share specific Information, such as your name and email address, with such business partner on your order form…..” Unfortunately, it continues with “… or (2) when Our business partner provides a product or service that We feel may be of interest to you.” That second part makes the assurance meaningless. The statement means that the company will share personally-identifiable information with anyone it chooses to do business with – or more bluntly, to whom it will sell prospects’ names for profit. Give them enough money and I’m sure that practically anything will seem interesting.

The lesson I draw from this cursory investigation is that no one can afford to do business with people who do not use the same strict policies of privacy protection as their own organization. Readers should perform a systematic audit of all their organizations’ links to third parties to verify that deviations from their privacy policies do not lead to embarrassment and legal liability.

The unacceptable site I located includes methods for opting out of the unwanted advertising and sharing of personally-identifiable information; that topic is the subject of the third article in this series.

* * *

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://www2.norwich.edu/mkabay/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.
In my most recent two columns, I’ve been discussing privacy policies. Today I want to look at some of the issues that can occur when you work with other organizations whose policies may differ from yours.

One of the sites I investigated where interested parties could fill in a form to request information included some information on opting out of receiving junk e-mail and other unsolicited marketing materials from itself, its business partners, and anyone to whom it chose to sell enquirers’ names.

The Privacy Policy included the following information:

- **E-mail Opt-out Options**: Each marketing e-mail We send includes instructions and an opt-out link.

- **Refusing Cookies**: Subject to the section below pertaining to cookies and web bugs, you have the ability to prohibit being served an advertisement based on cookie technology. We utilize reputable third-party vendors to serve advertisements. If however, you are not comfortable with cookies, you can adjust the settings within your browser to further prohibit being served a cookie. Please see the browser’s instructions to perform this task.

- **The National Advertising Initiative (NAI) has developed an opt-out tool with the express purpose of allowing consumers to "opt-out" of the targeted advertising delivered by its member networks. You can visit the NAI opt-out page and opt-out of this cookie tracking. Please visit: [http://www.networkadvertising.org/optout_nonppii.asp](http://www.networkadvertising.org/optout_nonppii.asp)**.

- **Other Options**: If you would like to opt-out of Our promotional marketing, and would like to contact Us, please send Us an e-mail at [privacy@<suppressed>.com](mailto:privacy@<suppressed>.com)

Most people in the security field with whom I have discussed the issue argue strongly against opting-out as an acceptable form of control over the abuse of personally-identifiable information. The European Coalition Against Unsolicited Commercial Email (EuroCAUCE) <[http://www.euro.cauce.org/en/](http://www.euro.cauce.org/en/) > has a succinct explanation of the arguments<[http://www.euro.cauce.org/en/optinvsoptout.html](http://www.euro.cauce.org/en/optinvsoptout.html) >; here is my summary of the issues:

- **Opt-out schemes cannot cope with the sheer scale of spamming.** Spreading e-mail addresses from one spammer to another inevitably outraces attempts to react to each new source after the fact.

- **It is impossible to ensure that permanent do-not-spam lists are consulted by spammers.**

- **There is no mechanism for supervision of compliance efforts.**
There are no enforcement mechanisms to prevent abuse.

In my view, opt-out schemes for protecting privacy are usually legitimate attempts to balance marketing departments’ needs for productivity with privacy advocates’ preference for better protection. However, for some unscrupulous marketers, opt-out policies may mask deliberate programs to capture user information that can be used or sold at a profit before the users can stop the abuse. Your organization should carefully examine the advantages and disadvantages of opt-out schemes before signing contracts with firms that use such methods.

My personal preference is to opt out of using opting out.

* * *

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://www2.norwich.edu/mkabay/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.
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@$string1>.com, mqkabay@$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:mekebay@gmail.com>; Web site at <http://www2_norwich.edu/mkabay/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.