SAGESSE

ISSN 2560-7014

ENHANCE COMMUNICATIONS TO IMPROVE PRIVACY PRACTICES

Anne-Marie Hayden
Communications & privacy consultant
Hayden Public Relations & nNovation LLP

ABSTRACT

Good communications are vital to organizations proactively meeting their privacy obligations. Certain techniques can also help manage privacy challenges when they inevitably arise. In this article, discover concrete techniques to better comply with consent and openness requirements and improve online privacy policies and notices. You'll also acquire practical crisis communications tips to plan for – and react to – a privacy breach.

INTRODUCTION

Guidance on consent, a hallmark principle in many privacy laws, often emphasizes that privacy notices and policies need to be offered in plain, easy-to-understand language for consent to be truly meaningful. The thing is, the regulators' guidance doesn't often tell you exactly *how* to do that. I've spent 25 years in communications and 18 of those in privacy. Now, I enjoy being a privacy and communications consultant and, in this role, I help organizations improve their privacy communications to enhance their compliance. This article flows from a presentation I made at the ARMA Canada Information Conference earlier this year (2021)[1]. Below, I share ideas on what I see as the links between privacy and communications. I also offer some concrete communications tips that can help, both in terms

[1] ARMA Canada Information Conference 2021, Integrating Communications for Improved Privacy Practices Tuesday, June 1, 2021, https://armacanada.org/home/information-conference/2021-on-demand/#

of avoiding some privacy challenges and in addressing privacy problems, like breaches, when they arise.

THE CONNECTION BETWEEN COMMUNICATIONS AND PRIVACY

Organizations are required to designate someone responsible for managing privacy. Some ARMA members are directly responsible for information privacy, access and, of course, records and information management. Even if you do not wear the chief privacy officer – or CPO – hat, good records management practices are fundamental to meeting privacy obligations and reducing privacy risks. Consider the important roles you play, along with others, in limiting access and in having safeguards, disposition schedules and methods for proper information disposal.

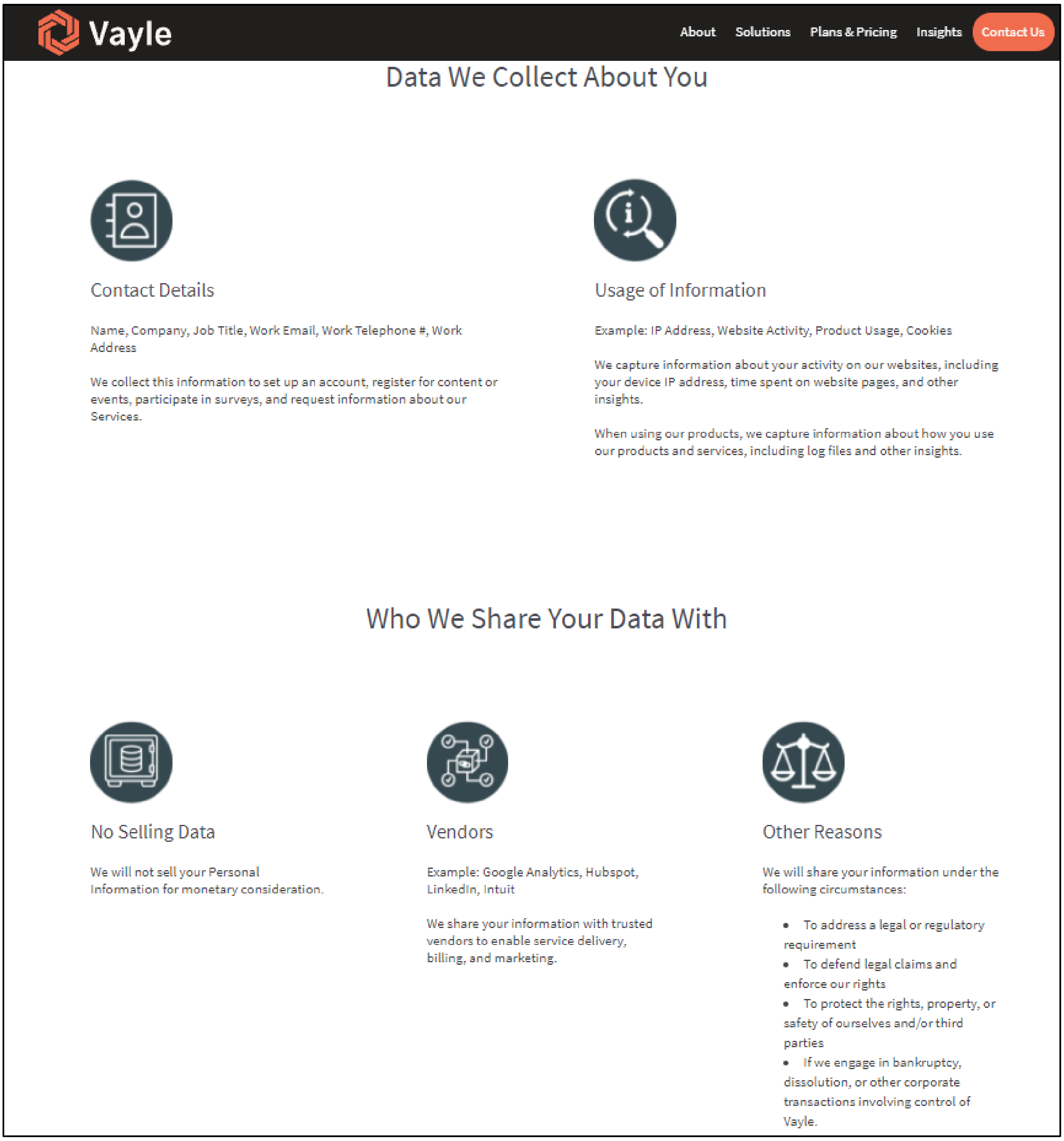
In addition to records and information management, communications is another important skill and function that can enhance your privacy practices. Whether in the public or private sector, when managing privacy, the 10 privacy principles, tucked into schedule 1 of the *Personal Information Protection and Electronic Documents Act* (PIPEDA), often come into play, either to comply with the legislation or to do a comprehensive privacy impact assessment (PIA). If you examine each of the principles closely, many of them (such as Accountability, Identifying Purposes, Challenging Compliance) have an interplay with communications. Here, I want to focus on the two most concretely related privacy principles: Consent and Openness.

CONSENT AND OPENNESS

There are, of course, differences between the public and private sectors insofar as how or when consent is involved[2]. At the core, however, both of these principles are about ensuring individuals are aware of, that they understand and that they have access to how their personal information is collected and used so that they can actively decide whether to hand it over.

[2] For more information on the Privacy Act go to https://laws-lois.justice.gc.ca/ENG/ACTS/P-21/index.html and for more information on PIPEDA go to https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/index.html

Privacy notices and policies play a role in obtaining meaningful consent. Privacy notices[3], like the one shown in Figure 1 highlights what personal information is collected, with whom it's being shared and for what purpose.



Data We Collect About You

Contact Details

Name, Company, Job Title, Work Email, Work Telephone #, Work Address

We collect this information to set up an account, register for content or events, participate in surveys, and request information about our Services.

Usage of Information

Example: IP Address, Website Activity, Product Usage, Cookies

We capture information about your activity on our websites, including your device IP address, time spent on website pages, and other insights.

When using our products, we capture information about how you use our products and services, including log files and other insights.

Who We Share Your Data With

No Selling Data

We will not sell your Personal Information for monetary consideration.

Vendors

Example: Google Analytics, Hubspot, LinkedIn, Intuit

We share your information with trusted vendors to enable service delivery, billing, and marketing.

Other Reasons

We will share your information under the following circumstances:

- To address a legal or regulatory requirement
- To defend legal claims and enforce our rights
- To protect the rights, property, or safety of ourselves and/or third parties
- If we engage in bankruptcy, dissolution, or other corporate transactions involving control of Vayle.

Figure 1 1 (Vayle, 2021)

[3] https://www.vayle.io/

Privacy notices need to be offered just-in-time, within the right context, and sensitive personal information requires express, opt-in consent. Privacy policies, meanwhile, are used to educate and train employees on an organization's privacy management practices. By making privacy policies public on a website, they support efforts to obtain consent and they demonstrate transparency, openness and accountability. Privacy policies tend to contain more detailed information about privacy practices including safeguards for protecting information, as well as contact information and procedures for accessing or correcting personal information, asking questions, or even making a complaint.

THE PROBLEM WITH PRIVACY POLICIES

This isn't breaking news, but there are a few challenges when it comes to privacy policies. For one thing, many businesses say they don't have a privacy policy[4]. Policies that do exist are not offered in context and they're often somewhat hidden. Another issue is that most people don't read these policies anyway[5], often due to how typically long and complex they can be.

Typical privacy policies are often filled with legalese. They continue to take, on average, ten minutes each to read and some say it would take three months each year to read all of the privacy policies connected to the services you use[6]. This is a barrier to obtaining meaningful consent.

It's no wonder then that very few Canadians say they understand what organizations are doing with their personal information[7]. And they're not alone. Employees also don't understand the privacy policies, so they are less capable of respecting them, not to mention answering questions about issues or practices.

It's not the easiest thing to do perfectly. There are real tensions between transparency and simplicity, finding just the right balance between the two.

[4] According to this survey, 65% of companies have a privacy policy, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2020/por_2019-20_bus/

[5] Just 9% of adults say they always read a company's privacy policy before agreeing to the terms and conditions, while an additional 13% say they do this often. And additionally, 38% of Americans say they sometimes read these policies. There is also a segment of the population who forgo reading these policies altogether: More than a third of adults (36%) say they never read a privacy policy before agreeing to it, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/

[6] https://www.npr.org/sections/alltechconsidered/2012/04/19/150905465/to-read-all-those-web-privacy-policies-just-take-a-month-off-work

[7] For example, only 3/10 Canadians say they have an understanding of what the federal government is doing with their personal information, https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2019/por_2019_ca/

TOP TEN TIPS FOR BETTER PRIVACY COMMUNICATIONS

Here, since many records and information management professionals play a role in protecting privacy, I share a few tips to help improve privacy communications, particularly in online privacy notices and policies.

1. *APPLY BEST PRACTICES IN WRITING FOR WEB*

Communicating online requires us to adapt the way we write things, so let's start by recognizing we are almost always writing for online. Given this, we need to consider how people obtain and digest that online content.

2. *KEEP IT SHORT*

Make sure your sentences are short and concise, with one key idea each. Keep trimming, re-reading and finding efficiencies in your text.

3. *USE ACTION WORDS*

Avoid the passive voice – action words resonate a lot better with audiences. An easy way to remember the difference: the active voice tells what a person or thing does. The passive voice tells what is done to someone or something. For example, "The privacy officer will describe the process" as opposed to "The process will be described to you by the privacy officer."

4. *MAKE IT CLEAR*

Most of us are guilty of using jargon, acronyms and abbreviations all too often in our day-to-day work with colleagues, but it's really important to eliminate them especially when communicating with the public, to ensure our content is understood. We often end up writing for ourselves, forgetting that we're not the audience!

5. *USE SUB-HEADINGS*

Use sub-headings to make your text scannable to the eye. Think of media headlines you may scan if you don't have time to read the whole thing. We read this way all day long, online, often without realizing it.

6. *MAKE LISTS*

Well-organized lists are also helpful at getting information across – on or offline. Use bullets and numbered lists instead of complete paragraphs.

7. FOCUS ON TOP TASKS

Lead with what web experts call the "top tasks." These are the main reason people go to a particular web page. Think about why people go to that page or site, what they likely want to accomplish, and give it to them right off the top. In media they say "don't bury the lead," so, similarly, don't put the key information at the end of the text you're writing for the web.

8. LAYER INFORMATION

Using layers to point to more in-depth information can be helpful, to go into more detail on something, again such as shown in Figure 1 from above. Think of how you could point to the more comprehensive privacy policy from the notice, for example.

9. HAVE TEXT REVIEWED

Ask someone who is less familiar with your subject matter to review your text and encourage them to give you honest feedback. You can even show it to your kid or your mom.

10. RUN CONTENT THROUGH READABILITY TESTS

Make sure a range of people can understand your content. Many writers don't realize that most word processing software has built in readability and accessibility tests. Recognize these tools have their limitations, but it's still useful to run your content through them, as you work to simplify and streamline your text. You may be surprised by the results and it may encourage you to further refine what you've written.

CRISIS COMMUNICATIONS FOR BREACHES

It's often not a question of *if* but rather *when* a breach will occur.

These tips can help avoid certain privacy problems, but they are not a silver bullet. They can't help if, for example, if you're collecting or using personal information when you shouldn't be. And they're not going to prevent a privacy breach.

Alexander Graham Bell wisely said that “Before anything else, preparation is the key to success.[8]” It’s a good idea – and an example of how to help address the Accountability and Safeguards principles – to be prepared with a breach readiness plan, before one occurs. A breach readiness plan is usually prepared by the Chief Privacy Officer, but often involves many parties across an organization, including records and information management.

It’s also a good idea to involve the communications folks to ensure a crisis communications section is included in this plan. It’s not necessarily fun to think of the things that can possibly go wrong, but for the purposes of that plan you will want to envisage and test various scenarios.

Identify and media train your potential spokespersons, so they’re ready, willing and most of all, able. And prepare some foundational key messages, as well as questions and answers, in advance, that you can refine further once something hits. The key is not to waste time, when a breach occurs, doing certain things you could have been ready with.

When a breach occurs, you need to quickly review and implement your organization’s breach plan. I encourage you to involve your communications colleagues in this process at all key stages. I’ve seen them too often be brought in at the last minute, too close to when it’s time to go live with an announcement. That’s not a way to ensure the organization is putting its best foot forward publicly.

You do need to get the facts related to the incident and find out about the impact and the legal issues. When it comes to notifying regulators or to the public, you’ll need to assess the requirements to do so, the scope and the impact of the incident and what information is available. From a communications’ point of view, you need to ensure you have very clear, concise and consistent messaging. You want to exhibit that you’re responsive, transparent and empathetic. I also urge you not to forget internal audiences, because consistency in messaging is key. This is a frequent issue for organizations.

Any organization that has experienced a breach knows that breaches are a little different from other types of crises, so it’s important to recognize this. They can often be like peeling an onion, as the situation evolves. Given this, you should assume there will be a series of communications and be ready to adapt as the situation evolves.

[8] Interview with Bell published in How They Succeeded (1901) by Orison Swett Marden

WHEN YOU'RE THE SPOKESPERSON

At times, there can be a role for information management (IM) and privacy experts to play in public communications and media strategies. Greater access to subject-matter experts can often enhance trust and increase that sense of an organization's accountability.

When should the privacy person be the spokesperson? It may depend on your organization's size, its internal policies and whether it is open to a decentralized approach. It may also depend on whether your privacy management program is at a certain level of maturity and generally in good shape. If, however, your organization's breach response plan identifies you as a possible spokesperson, you'll want to develop your media skills *before* a problem arises.

This means working with communications colleagues on key messages, as well as learning and practicing strategies to handle tough questions and to apply bridging techniques, which are ways you can move away from more difficult or controversial questions to ones you are more comfortable responding to. Remember when speaking to the media never speculate or repeat negatives, unless you want to see those words quoted in a news story.

It's a good idea to always over-prepare. Keep in mind that honing these skills can help, even if you are not playing a front-facing role with the media, but you just want to be more confident and comfortable – when, for example, you're dealing with media for other reasons, such as managing access to information requests.

COMMUNICATING TO BUILD TRUST

Privacy can sometimes be seen as standing in the way of communications activities. I believe we need to work on evolving this narrative and put privacy forward as a value proposition instead. Doing privacy well can directly improve credibility and trust[9]. What's exciting to see is that organizations are starting to get this, and some are reaping the rewards, as individuals say they prefer to work and do business with organizations that protect their privacy.

Privacy officers have made great strides over the years in making connections with Legal, Information Technology, Security, IM – and these professions have become part of the broader privacy community. It's less common to see communications practitioners in the

[9] https://www.forbes.com/sites/shamahyder/2021/06/22/how-to-use-data-while-maintaining-consumer-trust-what-the-latest-research-reveals/?sh=3d6ca7b42ddd

space; more headway could be made to tighten links between communicators and privacy officers. I would encourage you to start collaborating by learning and applying some communications best practices such as those highlighted earlier in this article.

Hopefully this article gives you some helpful ideas on why this is important, how good communications are vital to privacy compliance, what you can do in practical terms, and how communications can help manage privacy challenges when they do arise.

It's not a perfect science. Meanwhile, the channels we communicate through are changing all the time – and as my teenagers remind me every day, there are so many channels. Anyone who sends an email, drafts or explains a policy, makes a presentation, deals with clients or participates on social media has become a communicator of sorts, even if we'd prefer not to be. Luckily, these are very transferable skills.

This is also an opportunity for records and information management professionals to increase their communications expertise and, in tandem, bolster their organizations' privacy compliance. The best efforts at applying some best practices, even if imperfect, show real effort toward transparency, openness and accountability. And that's what garners trust and is a big win, from a privacy perspective.

ABOUT THE AUTHOR

Anne-Marie led communications for the federal privacy regulator for close to two decades. She combines her passion for privacy, knowledge of data protection and 28 years of communications expertise. She helps clients comply through, for ex., privacy impact assessments and clear privacy policies, and offers guidance on security breaches.