ENLASO®

ENLASO Best Practices White Paper
The Importance of Linguistic Discretion in the Age of Facebook

A White Paper by John Watkins
President and Chief Operations Officer
ENLASO Corporation
October 2011

BSI™
ISO 9001
FS 40617

This Page Intentionally Left Blank

Table of Contents

This Page Intentionally Left Blank

Abstract: *Non-Disclosure Agreements (NDA's) are commonly signed contracts among end customers, vendors, and linguists, but confidentiality is often misunderstood, especially in an age where the boundaries surrounding "private information" have become increasingly mutable. John Watkins, ENLASO's President and Chief Operating Officer, defines some of the boundaries regarding "confidential information", the risks to corporations and linguists if these boundaries are ill defined, and what measures should be taken at the bare minimum to protect customer information.*

Introduction

In the language services industry, Non-Disclosure Agreements (NDA's) are commonly signed contracts among customers, vendors, and linguists. Understanding the terms of the typical NDA and meeting the corresponding requirements to protect confidential information may be daunting to many people. By understanding the driving forces behind the need for confidentiality and developing ways to respect the confidentiality while performing our language services, all of us can rest more easily.

The boundaries of personal privacy are eroding in today's online world, both through active and passive changes. For many of us, online privacy was not on our RADAR a few years ago. The explosion of social media online has changed that. Now we readily have access to sites that release personal information—from the 140 characters on Twitter, to unfettered content on Facebook. Many of us now share with abandon and with little thought as to how personal data are used – at least until we fall prey to identity theft.

Our perception of what is personal and what is appropriate to share online has changed as a result of our easy access to social media. For example, I daresay that my expanding circle of "friends" know more about my political and social views, my sense of humor, my favorite foods, my hobbies, and my taste in music and art than even my closest family and friends did just five years ago. I include photos, video clips, and articles that support my views for the world to see. Even online shopping is integrated with social media. As a result, I have provided my address, phone number, mother's maiden name, credit card number, birth date, and other personal information many times, doing everything from shopping on Amazon to ordering coupons through Facebook. My shopping history on a variety of sites happily helps companies tailor their offerings to me, sharing their information with "trusted partners" so that I now see ads for discounts at local spas and restaurants in my home town and, perhaps most alarmingly, a recent invitation to join the AARP (What? The American Association of Retired Persons wants me? How can that be? I won't be able to retire for 30 more years, what with the market upheavals. I found out, after calming down, they take members at 50. Thank you, but I am not quite there yet).

Mark Zuckerberg had it right when discussing the rollback of Facebook's privacy controls, when he said that "these are the social norms now..."[i] Indeed, the recent launch of Google+ resulted in a policy change that plots the demise of private Google profiles.[ii]

Privacy for Language Services Providers

You might think that this shifting perception of personal privacy would affect how companies feel about their own privacy, that they would be as eager to share as they are to have us share. You would, though, be wrong. While the companies are delighted to exploit the personal data they mine from our online presence to better market their wares and services to you, they fiercely guard their proprietary information to better compete in the marketplace.

Just a little thought clarifies that we, as language services providers, are privy to a wide variety of corporate secrets in our day-to-day work. Here are a few examples, can you think of more?

- **Target Markets**: When a medical device manufacturer is releasing a new blood scanner in 12 markets, we are translating their content for each of those markets and have direct knowledge of which markets are being targeted.
- **Product Functionality**: We are among the first to know about new functionality in products, seeing it before it is released (often before release in the US as well).
- **Target release dates**: Our work is always under time pressure, because our customers' marketing departments have set confidential release dates for their products that they strive to meet (and pass that requirement on to us).
- **Proprietary methodologies**: Sometimes our customers have developed proprietary processes for product development and we may be privy to those processes through the content we translate.
- **Legal issues**: Many of us provide legal translations of customer contracts, employment agreements, patents, property leases, litigation settlements, and other highly confidential information.

Beyond these examples of confidential information for our customers' business content, we also may see data from their own customers – personally identifiable data of the users of their services or products. Personally identifiable data are protected in various ways by federal and state law (or, just as importantly, the privacy laws of the target countries). We see this type of data in language services more frequently than you might expect. It occurs as the result of translating customer support content in the medical industry or providing interpretation between customer service representatives in, for example, the medical insurance industry and their customers who have limited English speaking skills. Working with human resource departments also exposes us to these data. Even technical services help desks often receive these data.

Understanding Non-Disclosure Agreements

We know that we receive confidential information from our customers and, most likely, we have agreed to protect each customer's confidential information. By better understanding the agreements we sign, we are better able to protect their confidential information.

Non-Disclosure Agreements (NDAs) are contracts that are entered into by two or more parties where these parties agree to certain parameters about the transfer of confidential information. Parties are typically the customer, who has the confidential information, and the other people (parties) who may have access to that confidential information in providing services to the customer. NDAs may be either unilateral, where the agreement controls the transfer of confidential data from only one party to the other party and thereby disregarding transfers from the other party, or they may be bilateral, where the agreement controls the transfer of confidential data from the two parties signing the agreement.

Let's use a concrete example to understand where the multilateral and unilateral NDAs come into play. OmniTex LTD developed the revolutionary CleanDome Digital Chlorine Monitor and Dispenser. This is the first such device on the market and they are excited to launch it in the US and five other international markets: Mexico, Brazil, Spain, Italy, and France – the pool-loving countries. They need to localize content that corresponds to distribution agreements with the five target markets, a user guide, a quick start guide, a software user interface, and a reporting tool that monitors and reports on their chlorine levels and chemical utilization. They come to ENLASO, a multi-language service provider, for localization of their content into the five markets. ENLASO and OmniTex sign a bilateral NDA that protects OmniTex's confidential information and, at the same time, ENLASO's proprietary service methodology and pricing. To perform the services for OmniTex, ENLASO has to provide content to subcontracting linguists working on the OmniTex project, so ENLASO has a unilateral NDA with each of the linguists

that ensures that both OmniTex's and ENLASO's confidential information is protected by each linguist.

Fortunately, NDAs are pretty consistent despite obvious wording differences. They cover the same content, more or less, in their efforts to protect confidential data. An NDA typically achieves this by defining the following items:

- The parties, defined with the legal names and corresponding addresses. Legal entities may be companies, organizations, individuals, or other defined entities.
- The nature of the confidential information (for one or both parties). Typically, this includes proprietary business processes, methodologies, functionality, pricing, scheduling, content, and any other identified trade secrets. Confidential information does not include situations where the recipient has prior knowledge of the material, the recipient learns of the confidential information from another source, or the materials are available to the public.
- The purpose(s) for the disclosure of the confidential information. In the language services, this is typically for the provision of translation, localization and/or interpretation services (and other related services, such as internationalization).
- The term of the agreement, typically in years. This defines the period during which confidential information may be distributed.
- The term that information is to remain confidential, typically in years. This defines the period that the recipient of confidential information must keep the information confidential (and is usually longer than the term of the agreement).
- The obligations of the recipient of the confidential information. These may include using the material only for the defined purposes, disclosing the confidential information only to those other parties with a need to know (who are bound by a similar NDA between the recipient and the third-parties), and to use reasonable efforts to keep the information secure. Pay careful attention to this section if you are the service provider. Often this restricts distribution to any third parties. If this is so, you would need to modify the agreement if you need to transmit the information to your own third-party subcontractors to perform the services.
- The provisions for permissible disclosure. These typically involve disclosure by law or court order.
- The permission to obtain ex-parte injunctive relief. This means that, if the receiver inappropriately discloses confidential information as defined by the agreement, the owner of the confidential information may obtain an equitable remedy in the form of a court order that requires the receiver to refrain from disclosing the information. Failure to do so would leave the receiver who discloses confidential information may result in criminal or civil penalties.

Note that the translations you provide under contract to your customers are usually defined as the intellectual property of the customer and thereby protected by the non-disclosure agreement as well.

Risks to Disclosure

Now that we have a clearer understanding of the requirements of Non-Disclosure Agreements, it is time ensure that we do not violate the terms. We hear frequently, especially in current news, about the intentional release of confidential information. Take, for example, the intentional hack into the Sony servers, putting at risk confidential user data of countless Playstation customers.[iii] We are not hackers and we do not intend to release our customers' confidential information; however, it is too easy to accidentally release confidential information if we are not paying attention.

As none of us are interested in exploiting confidential information for our own gains, we focus here on those accidental, or inadvertent, releases. Some of the processes we use in the language services industry provide opportunities for such accidental transmissions of confidential information. While we cannot provide legal advice, we can give you pointers of good practices that help avoid security breaches.

Data Transmission – You've Got Mail

The one tool used by all of us, every day, is email. Email provides an easy vehicle for accidently releasing confidential data. At one time or other, we have all tried to send an email to one recipient only to find out later it was sent to another, unintended recipient. You might want to send an email to joesmith@abc.com but when you typed in "Joe" in your "To:" field, joesmith@xyz.com populates the field. You hit send, not catching the mistake, and get a reply back from Joe at xyz saying "did you mean to send this to me?" For this reason, transferring customer content should be handled thoughtfully.

Business confidential information (as opposed to personally identifiable information), may be successfully transmitted by regular email if it is permitted under the terms of the NDA. A good way of knowing this is if the customer sends it to you via regular email. Remember, though, to check your recipient list to ensure only those who should receive the email do in fact receive it.

If required by your customer, using a secure FTP site provides the easiest way to securely transfer information. Note, thought, that under no circumstances should you receive files from a secure FTP server only to then distribute them outside your computing network with regular email. Doing so downgrades the security used and may put you at risk for inadvertently disclosing confidential information.

If your work requires you to handle personally identifiable information (say, translating employee application forms or medical claim forms), you need special precautions. Personally identifiable data includes names, birth dates, birthplaces, social security numbers or other national ID numbers, driver's license numbers, credit card numbers, and IP addresses. Never use regular email to transmit personally identifiable information. Any breach of security with these data requires exceptional efforts to mitigate the release. Personally identifiable information should only be transmitted via secure channels, such as encrypted email, encrypted attachments, or a fully secured FTP. Better yet, work with the owner of the data to "redact" or "strip out" the personally identifiable information before the data are sent to you and the translation process begins.

Translation Memories

Translation memories have revolutionized the language services industry, reducing the cost of repetitions and 100% match translations while reducing translation times and improving the consistency of the translation. Having more segments in the translation memory provides more opportunities for matches, reducing the translation timeline and costs. The natural result is the bigger the translation memory, the better.

If you have an NDA with a customer and you use a translation memory tool, the resulting translation memory is the confidential information of that customer. Say, for example, you have two customers who make blood glucose testing devices. It might be really tempting to use your TM from Customer A on the work for Customer B, but doing so would violate the NDA that you signed with Customer A. You should segregate your translation memories by customer to ensure compliance with signed NDAs.

There are, of course, exceptions. Some customers are eager to work together to exploit the savings a bigger TM for the subject matter provides. You, though, should not make that decision for them. If you think you can save your customer time and money, discuss this with them and get written permission from all parties before you combine translation memories.

Machine Translation

Anecdotally, using machine translation tools to facilitate human translation is gaining in popularity (but there are not many linguists who admit to it publicly). It is so easy now to pop in a paragraph on Google Translate or Microsoft Translator and obtain a translation that is often usable to the linguist in expediting the translation—it provides a "fuzzy" match of some quality level that may be refined. More sophisticated users may even integrate their translation memory workflow with machine translation, submitting unmatched segments through a machine translation API for those unmatched segments.

Unfortunately, as with sharing translation memories, submitting content to online machine translation tools poses a risk to protecting your customers' confidential information. Depending upon the tools you use, the settings you select, and the specific license agreement, you may see terms of the machine translation agreement such as: "(by) submitting or creating your content through the Service, you grant permission to use your content to improve or make available [the machine translation services]..." While the machine translation provider may not exploit the translated segments for anything other than improving the machine translation, the confidential content found in your segments may in fact be propagated into other products that then reuse the translated segment, thereby breaking confidentiality. The content is not yours, so you cannot grant the right to anybody else to do something with that content.

As a result of the ambiguity regarding the release of confidential information while using machine translation, you should obtain permission in writing from your customer before submitting their content to an online machine translation service. Today, we find customers who are looking for ways to reduce their costs and, with appropriate education from you, they are often willing to "take the risk" of releasing segments to an online machine translation service to reap the corresponding benefits.

Oops – What to Do When You Release Data

Despite our best intentions, we may inadvertently release data. Sending an email to your customer about the successful receipt of files for translation but accidentally including somebody from another company on the recipient list is a relatively harmless mistake—unless the two parties are competitors. You can probably chuckle to yourself and send a corrective email that explains the problem to both parties. Just be sure to remove the unintended recipient from the email chain going forward.

If, though, you transmitted confidential data, which could be anything from a customer's translated user manual to an excel spreadsheet containing personally identifiable information (such as name, birth date, and social security number), you have certain obligations to follow.

- Notify the customer of the breach in security, explaining the circumstances.
- Work with the customer to make a good faith effort to mediate the disclosure. For example, discussing with the unintended recipient that the content is confidential and must be destroyed immediately, asking for a confirmation of destruction from the recipient. Your customer may require additional actions based upon the nature of the information disclosed.

Note that the intentional disclosure of confidential information carries the risk of grave consequences with a host of additional penalties. These penalties include both criminal penalties and imprisonment as well as separate civil penalties. For example, HIPAA sanctions for disclosing medical information are as follows:

- Civil penalty of $100 to $50,000 per violation, capped at $1.5M for the year.
- Criminal penalties of $100,000 and up to 5 years imprisonment for release under false pretenses and $250,000 in penalties and up to 10 years imprisonment for disclosure with intent to sell, the transfer or use for commercial advantage, the transfer for personal gain, or the transfer resulting in malicious harm.

Next Steps

When you get home, use your knowledge to review the NDAs you have signed, taking the time to ensure your workflow processes have the steps necessary to protect your customers' confidential information. With just a little planning and thoughtful execution, you can adhere to the requirements of each NDA while providing great service to your customers. You can, indeed, rest a bit easier knowing you have done what you can to protect the confidential information.

---

[i] Kamer, Foster. "Facebook's Mark Zuckerbert on Your Erased Privacy: "There Are the Social Norms, Now," in *Gawker* (http://goo.gl/Yg6ss), January 10, 2010.
[ii] Weinberger, Matt. "All Google Profiles will be public...," in *ZDNET* (http://goo.gl/CYyPr), July 6, 2011.
[iii] Stevens, Tim. "Sony provides PSN update, confirms a 'compromise of personal information' (updated)," in *endgadget* (http://goo.gl/DFycr), April 26, 2011.