# Confidentiality in Translation: Translator and Interpreter Legal and Ethical Obligations

Israel Translators Association

2018 Annual Conference – Tel Aviv

Presented by Emanuel Weisgras, Esq.
Founder and CEO of Weis Words International Translations
www.weistrans.com

**Translators, especially translators in specialty fields such as law, medicine, and finance, are often exposed to their clients' most important secrets and confidential information.**

**This discussion will seek to review translators' legal and ethical obligations to maintain the confidentiality of source and translated materials, based on requirements and guidelines in the US, the EU, and the Middle East.**

**It will also discuss common confidentiality pitfalls such as machine translation, free email accounts, and peer support platforms.**

# EMANUEL WEISGRAS

Emanuel@weistrans.com

www.weistrans.com

WEISWORDS
International Translations

Goldfarb Seligman
Law Offices | Established 1930

CARDOZO LAW
BENJAMIN N. CARDOZO SCHOOL OF LAW • YESHIVA UNIVERSITY

NYU | COLLEGE OF ARTS & SCIENCE

FIRE DEPARTMENT CITY OF NEW YORK

DISTRICT ATTORNEY NEW YORK COUNTY 1625

POLICE DEPARTMENT CITY OF NEW YORK

**DISCLAIMER** (of course!)

***All materials have been prepared for general information purposes only. The information presented during this session is not legal advice, is not to be acted on as such, may not be current and is subject to change without notice.***

**No Attorney-Client Relationship or Legal Advice**

Communication of information during this session and your receipt or use of it (1) is not provided in the course of and does not create or constitute an attorney-client relationship, (2) is not intended as a solicitation, (3) is not intended to convey or constitute legal advice, and (4) is not a substitute for obtaining legal advice from a qualified attorney. You should not act upon any such information without first seeking qualified professional counsel on your specific matter. The hiring of an attorney is an important decision that should not be based solely upon the information provided during this lecture.

Unless otherwise noted, all materials, including but not limited to images, illustrations, designs, icons, photographs, video clips, software, and written and other materials that are part of this presentation are protected under copyright laws and are the trademarks, trade dress and/or other intellectual properties owned, controlled or licensed by Emanuel Weisgras and/or Weis Words International Translations. No part of these materials may otherwise be copied, reproduced, stored, republished, uploaded, posted, transmitted, or distributed in any form or by any means, electronic or mechanical, now known or hereafter invented, without the prior written permission from Emanuel Weisgras and/or Weis Words International Translations.

# "CONFIDENTIALITY" DEFINED

Black's Law Dictionary – 7th Edition:

- Confidentiality, *n*. 1. Secrecy; the state of having the dissemination of certain information restricted.

Oxford English Dictionary:

- Confidentiality: The state of keeping or being kept secret or private.
- Related – secret, privileged.

# WHY IS CONFIDENTIALITY IMPORTANT?

1. Protect private personal information
2. Private medical information
3. Commercial and trade secrets
4. Criminal investigations
5. Government secrets/national security

# WHAT IS (USUALLY) PROTECTED BY CONFIDENTIALITY

Any non-public material provided by the client. May include source material (documents, recordings, conversations), support material, translated material, and email correspondence.

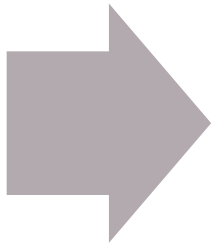
Risks of breach to confidentiality are everywhere, often hidden in plain sight.

# WHO OWES A DUTY OF CONFIDENTIALITY AND TO WHOM?

- Duty may be owed by: Language Service Providers (LSP), translators/interpreters, any subcontractors
- Duty owed to client or employer: LSP, oursourcing linguist, and of course the END CLIENT

# WHO BEARS THE RESPONSIBILITY/LIABILITY FOR MAINTAINING CONFIDENTIALITY?

Agency, Freelancer, Subcontract, Client?



Who is subject to an obligation?

- Applicable law
- NDA
- Secondary obligation (work done for a law firm)
- Storage of client material: secure? Statutory requirements?

- Laws and Statutes
- Codes of Ethics
- Local and International Standards (ISOs)
- Contracts and Agreements

# SOURCES OF OUR OBLIGATIONS:

# LEGAL AND STATUTORY SECRECY REQUIREMENTS

# ISRAEL PRIVACY PROTECTION LAW OF 1981

2. An infringement of privacy constitutes one of the following:

- (5) copying the contents of a letter or other scripts not intended for publication, or the use of contents thereof, without the permission of the addressee or the writer, unless the script is of historical value and no more than fifteen years have passed since the time when it was written; for this purpose, script – including an electronic message as defined in the electronic signature Law, 2001;
- (7) infringement of duty of confidentiality prescribed by law in respect of a person's private affairs;
- (8) infringement of duty of confidentiality in respect of a person's private affairs, whether it was explicitly or implicitly prescribed in an agreement;
- (9) use or passing on of information on a person's private affairs, for a purpose other than which was prescribed;
- (10) publication of or the passing of anything that was obtained by way of an infringement of privacy under paragraphs (1) to (7) or (9);
- (11) publication of any matter that relates to a person's intimate life, including his sexual history, or state of health or conduct in the private domain.

# US ESPIONAGE ACT OF 1917

18 U.S. Code § 793:

- **(d)** Whoever, lawfully having possession of, access to, control over, or being entrusted with any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted or attempts to communicate, deliver, transmit or cause to be communicated, delivered or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it on demand to the officer or employee of the United States entitled to receive it; or
- **(e)** Whoever having unauthorized possession of, access to, or control over any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, or note relating to the national defense, or information relating to the national defense which information the possessor has reason to believe could be used to the injury of the United States or to the advantage of any foreign nation, willfully communicates, delivers, transmits or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it; or
- **(f)** Whoever, being entrusted with or having lawful possession or control of any document, writing, code book, signal book, sketch, photograph, photographic negative, blueprint, plan, map, model, instrument, appliance, note, or information, relating to the national defense, (1) through gross negligence permits the same to be removed from its proper place of custody or delivered to anyone in violation of his trust, or to be lost, stolen, abstracted, or destroyed, or (2) having knowledge that the same has been illegally removed from its proper place of custody or delivered to anyone in violation of its trust, or lost, or stolen, abstracted, or destroyed, and fails to make prompt report of such loss, theft, abstraction, or destruction to his superior officer— Shall be fined under this title or imprisoned not more than ten years, or both.

# US HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT OF 1996 (HIPAA)

- **Protected Health Information.** The Privacy Rule protects all "*individually identifiable health information*" held or transmitted by a covered entity or its business associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "protected health information (PHI)."[12]
- "Individually identifiable health information" is information, including demographic data, that relates to:
- the individual's past, present or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual,
- and that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).

(from HHS.gov – HIPAA Security Summary)

# UK – OFFICIAL SECRETS ACT OF 1989

- **8 Safeguarding of information.**
- (1)Where a Crown servant or government contractor, by virtue of his position as such, has in his possession or under his control any document or other article which it would be an offence under any of the foregoing provisions of this Act for him to disclose without lawful authority he is guilty of an offence if—
- (a)being a Crown servant, he retains the document or article contrary to his official duty; or
- (b)being a government contractor, he fails to comply with an official direction for the return or disposal of the document or article,
- or if he fails to take such care to prevent the unauthorised disclosure of the document or article as a person in his position may reasonably be expected to take.
- (2)It is a defence for a Crown servant charged with an offence under subsection (1)(a) above to prove that at the time of the alleged offence he believed that he was acting in accordance with his official duty and had no reasonable cause to believe otherwise.
- (3)In subsections (1) and (2) above references to a Crown servant include any person, not being a Crown servant or government contractor, in whose case a notification for the purposes of section 1(1) above is in force.
- (4)Where a person has in his possession or under his control any document or other article which it would be an offence under section 5 above for him to disclose without lawful authority, he is guilty of an offence if—
- (a)he fails to comply with an official direction for its return or disposal; or
- (b)where he obtained it from a Crown servant or government contractor on terms requiring it to be held in confidence or in circumstances in which that servant or contractor could reasonably expect that it would be so held, he fails to take such care to prevent its unauthorised disclosure as a person in his position may reasonably be expected to take.
- (5)Where a person has in his possession or under his control any document or other article which it would be an offence under section 6 above for him to disclose without lawful authority, he is guilty of an offence if he fails to comply with an official direction for its return or disposal.
- (6)A person is guilty of an offence if he discloses any official information, document or other article which can be used for the purpose of obtaining access to any information, document or other article protected against disclosure by the foregoing provisions of this Act and the circumstances in which it is disclosed are such that it would be reasonable to expect that it might be used for that purpose without authority.
- (7)For the purposes of subsection (6) above a person discloses information or a document or article which is official if—
- (a)he has or has had it in his possession by virtue of his position as a Crown servant or government contractor; or
- (b)he knows or has reasonable cause to believe that a Crown servant or government contractor has or has had it in his possession by virtue of his position as such.

# CONFIDENTIALITY IN OUR PROFESSIONAL CODES OF CONDUCT

MOST, IF NOT ALL OF US, ARE MEMBERS OF PROFESSIONAL GUILDS AND ORGANIZATIONS.

MANY - PERHAPS MOST - HAVE PROFESSIONAL CODES OF CONDUCT THAT REAL WITH OUR OBLIGATIONS TO PRESERVE CONFIDENTIALITY

# ISRAEL TRANSLATORS ASSOCIATION - CODE OF ETHICS

I. **As a translator, interpreter and/or editor**, a bridge for ideas from one language to another and one culture to another, I commit myself to high standards of performance, ethical behavior, and business practices.

5. I will safeguard the interests of my clients as my own and divulge no obviously confidential information, and am aware that clients may condition my work on the signing of an NDA (non-disclosure agreement).

ISRAEL TRANSLATORS ASSOCIATION
אגודת המתרגמים בישראל
جمعية المترجمين الإسرائيلية

# ATA CODE OF ETHICS AND PROFESSIONAL PRACTICE § 2

We the members of the American Translators Association accept as our ethical and professional duty

2. to hold in confidence any privileged and/or confidential information entrusted to us in the course of our work;

ata
American
Translators
Association

# CHARTERED INSTITUTE OF LINGUISTS CODE OF CONDUCT

6.4 Members/Chartered Linguists will take all reasonable precautions to keep information and material provided by clients/employers confidential and secure (except where disclosure is required by law). This requirement will also apply to members/Chartered Linguists to whom part or all of a job is sub-contracted.

6.5 Members/Chartered Linguists will not use information acquired in the course of their work to gain unfair advantage or to disadvantage their client/employer. In particular, they will not solicit work directly from end clients for whom they have worked through an agency. Any member who is approached by such an end user with a view to working directly for him/her will inform the agency immediately.

# INSTITUTE OF TRANSLATION AND INTERPRETING - CODE OF CONDUCT

PRINCIPLE 3 – CLIENT CONFIDENTIALITY AND TRUST

1. CONFIDENTIALITY

1.1 Members shall maintain complete confidentiality at all times and treat any information that may come to them in the course of their work as privileged information, not to be communicated to any third party without prior written authority. They shall also require all those assisting them in their work to be similarly bound.

1.2 No member shall derive any gain from privileged information acquired in the course of work undertaken.

1.3 No member shall disclose privileged information about other members.

Institute of Translation & Interpreting

# CONTRACTUAL SOURCES FOR THE DUTY OF CONFIDENTIALITY

The Non-Disclosure Agreement (not to be confused with the non-compete agreement).

- Client NDAs (provided to us)
- Subcontractor NDAs (provided by us)

A subcontractor NDA should be as comprehensive as a client NDA (otherwise, by definition, the subcontractor puts us at risk of breaching our contractual obligations)

# NON-DISCLOSURE AGREEMENTS

CLIENT NDA'S AND SUBCONTRACTOR NDA'S

**“I’m afraid you will have to sign a non-disclosure agreement.”**


# CONTENT OF AN NDA

## What should appropriately appear in an NDA?

- Data security requirements: method of storage, destruction of material upon completion, future liability, etc. (neither wise nor always possible)
- Possible terms:

1. Non disclosure of confidential client information **unless authorized or required by law**
2. Not to gain commercial benefit
3. Data security
4. "Trickle down" obligations (use of subcontractors, etc.)

## What should not be in an NDA?

- Clauses that bind you to absolute secrecy
- Anything illegal or unethical
- Draconian penalty clauses

## Other considerations:

Professional privilege: when working for professionals who are subject to privilege/confidentiality requirements, does that privilege extend to linguists?

# WHEN PRIVILEGED INFORMATION IS NO LONGER PRIVILEGED

In certain cases, disclosure of confidential information may be required by law. Possible reasons may include:

1. Evidence of criminality (past, ongoing, or future).
2. Threat of imminent injury or death (i.e. suicidal ideations, death threats, etc.). This will often intersect with "evidence of criminality."
3. Required by judicial or quasi-judicial order.

So if we know that there is confidential information whose release can prevent a threat of death or injury, or ongoing criminality, that means we can disclose the information without fear of repercussions, right?

**WRONG!**

# THE CURIOUS CASE OF BETSY BENJAMINSON

- In 2010 - Betsy Benjaminson, a Japanese>>English technical translator was hired by a US based LSP to translate documents for Toyota's legal counsel.
- **High price but no regrets for Israel's gutsy Toyota whistle-blower**

**Translator Betsy Benjaminson -- 'a gnat biting the elephant's toe' -- has lost half her income since speaking up in an auto maker's fatal sudden-acceleration scandal**

- What would YOU have done?

# HOW LONG MUST WE KEEP THESE SECRETS SECRET?

Duration: Secrets don't naturally expire on a fixed date!

We should maintain confidentiality ALWAYS or as long as we are legally, ethically, and/or contractually bound to do so.

Sometimes, NDA's will specify the duration of the confidentiality obligation.

More likely, an NDA will remind us that SECRETS DON'T EXPIRE, but may stop being secret for other reasons.

# POSSIBLE PENALTIES FOR BREACH

Civil liability
Criminal liability
Professional censure
Loss of revenue/income

# WHAT IS USUALLY NOT PROTECTED BY CONFIDENTIALITY?

1

Anything already in the public domain

2

Anything that enters the public domain (and not through the linguist)

# HIDDEN DANGERS!!!

# HIDDEN (AND NOT SO HIDDEN) DANGERS

- Machine Translation (MT)
  - MT platforms such as Google Translate, Bing, Morfix
  - MT Plug-ins in CAT software
- Professional Forums
  - Proz.com – Kudoz
  - Facebook groups
  - Professional listserves
- Shared cloud workspaces:
  - Google docs, etc

# Google Privacy & Terms

- Google Translate and Google's Terms of Service:

**Your Content in our Services**

Some of our Services allow you to upload, submit, store, send or receive content. You retain ownership of any intellectual property rights that you hold in that content. In short, what belongs to you stays yours.

When you upload, submit, store, send or receive content to or through our Services, you give Google (and those we work with) a worldwide license to use, host, store, reproduce, modify, create derivative works (such as those resulting from translations, adaptations or other changes we make so that your content works better with our Services), communicate, publish, publicly perform, publicly display and distribute such content. The rights you grant in this license are for the limited purpose of operating, promoting, and improving our Services, and to develop new ones. This license continues even if you stop using our Services (for example, for a business listing you have added to Google Maps). Some Services may offer you ways to access and remove content that has been provided to that Service. Also, in some of our Services, there are terms or settings that narrow the scope of our use of the content submitted in those Services. Make sure you have the necessary rights to grant us this license for any content that you submit to our Services.

Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection. This analysis occurs as the content is sent, received, and when it is stored.

# COMMON FAUX PAS

LSP and outsourcing faux pas: sending out confidential material to numerous providers, many of whom haven't signed an NDA

# POTENTIAL CONFIDENTIALITY ISSUES

- Will your duty of confidentiality place you in an ethical or legal dilemma? (Disclosure of material that may not be legal or ethical may still place you at risk of liability).
- Liability insurance in case of claim of breach?
- Where do you work physically?
    1. Who has access to your: computer (who can see over your shoulder), desk, cell-phone, etc.
    2. Confidentiality applies everywhere. Who can hear us when we speak to others?
    3. Who can see over our shoulder to read what's on our screen?
    4. Share spaces such as WeWork
    5. Shared wi-fi (public wi-fi)
- Legal obligations to report: crimes, court orders, etc.

# DATA SECURITY AND PROTECTION

## "THE CLOUD"

Many of us use cloud storage, and with good reason. But is it secure? Does it protect our confidential materials?

# 1. WE GIVE UP AND HAVE NO CONTROL OVER OUR DATA!

Data is typically taken outside of the company's IT environment, and that means that the data's privacy settings are beyond the control of the enterprise. Because most cloud services are designed to encourage users to back up their data in real-time, a lot of data that wasn't meant to be shared can end up being viewed by unauthorized personnel as well. The best way to avoid such a risk is by ensuring you're your provider encrypts your files during storage, as well as transit, within a range of 128 to 256-bit.

# 2. DATA LEAKAGE

The cloud is a multi-user environment, wherein all the resources are shared. It is also a third-party service, which means that data is potentially at risk of being viewed or mishandled by the provider. Best strategy is to depend on file encryption and stronger passwords, instead of the cloud service provider themselves.

# 3. BYOD - BRING YOUR OWN DEVICE

BYOD brings significant security risks if it's not properly managed. Stolen, lost or misused devices can mean that a business' sensitive data is now in the hands of a third-party who could breach the company's network and steal valuable information. Discovering a data breach on an external (BYOD) asset is also more difficult, as it is nearly impossible to track and monitor employee (or contractor) devices without the proper tools in place.

# 4. SNOOPING

Files in the cloud are among the most susceptible to being hacked without security measures in place. The fact that they are stored and transmitted over the internet is also a major risk factor. And even if the cloud service provides encryption for files, data can still be intercepted on route to its destination. The best form of security against this threat would be to ensure that the data is encrypted and transmitted over a secure connection, as this will prevent outsiders from accessing the cloud's metadata as well.

# 5. KEY MANAGEMENT

The management of cryptographic keys has always been a security risk for enterprises, but its effects have been magnified after the introduction of the cloud, which is why key management needs to be performed effectively.

# 6. CLOUD CREDENTIALS

The basic value proposition of the cloud is that it offers near-unlimited storage for everyone. This means that even an enterprise's data is usually stored along with other customers' data, leading to potential data breaches via third parties. This is mitigated - in theory - by the fact that cloud access is restricted based on user credentials; however those credentials are also stored on the cloud and can vary significantly in security strength based on individual users' password habits, meaning that even the credentials are subject to compromise. While a credential compromise may not give attackers access to the data within your files, it could allow them to perform other tasks such as making copies or deleting them. The only way to overcome this security threat is by encrypting your sensitive data and securing your own unique credentials, which might require you to invest in a secure password management service.

# OTHER CLOUD STORAGE ISSUES AND PHYSICAL SECURITY OF EQUIPMENT AND DIGITAL MEDIA

In addition to the 6 issues we discussed, remember that in the end, commercial cloud storage services are not perfect and must constantly balance the need for security with costs and speed. **NOBODY IS PERFECT.**

Commercial cloud storage services are also theoretically susceptible to common hacking attacks such as DoS attacks, that may render your information inaccessible.

Be aware of your provider's security features. What level of encryption does it use?

Use secure passwords that you change frequently: at least 16 characters, mix of numbers, symbols, and upper and lowercase letters.

Try to use a service requiring two step verification.

Make sure your physical device is secure!

Consider additional encryption such as Boxcryptor and/or password protection for sensitive documents.

Consider email and/or desktop notifications whenever a device is added to your account or a file is changed.

## DOES THAT MEAN I SHOULDN'T USE DROPBOX, ONEDRIVE, OR GOOGLE DRIVE?

# SOME FINAL THOUGHTS

Be aware of your confidentiality obligations and the dangers to it.

Keep your clients' and even your own data secure

Tips on Data Protection:

- Avoid public computers and networks (Starbucks Wi-Fi, etc)
- Secure password, protected home/office networks
- Strong mobile device security including password/fingerprint security.

# QUESTIONS?

# CONTACT ME:

WEISWORDS
International Translations

Email:
Emanuel@weistrans.com

Visit our website:
www.weistrans.com

Twitter:
@WeisWordsTransl

Facebook:
www.facebook.com/WeisWords/