The Seven Deadly Sins of U.S. and non-U.S. software companies under U.S. export controls and sanctions laws


The recent $750,000 fine imposed by BIS against Intel subsidiary Wind River Systems for unlicensed software exports has drawn renewed attention to this oft-overlooked area of regulation and compliance. Rich Matheny and Jacob Osborn examine the deadly sins of the U.S. and non-U.S. software exporter.

Companies that make software or provide software-as-a-service ('SaaS') confront U.S. export control and economic sanctions laws from an unusual perspective. Their dynamic offerings and distribution models often clash with laws that cling persistently to a 20th century model, under which an 'export' means a physical box moving on a plane, truck, train, or vessel, across sovereign boundaries, to be unpackaged by customers that are fixed and knowable.

Compliance is a constant challenge, and the recent imposition by the Bureau of Industry and Security ('BIS') of a $750,000 fine against Intel subsidiary Wind River Systems for unlicensed software exports draws renewed attention to this regulatory area.

Focusing on software and SaaS distribution models, this article looks at recurring compliance 'sins' committed by companies whose activities are regulated by the Export Administration Regulations ('EAR') administered by BIS, of the U.S. Department of Commerce, and by the U.S. economic sanctions administered by the Office of Foreign Assets Control ('OFAC'), of the U.S. Department of the Treasury. These laws of course apply to U.S.-based software companies, but non-U.S. software companies increasingly find themselves at odds with U.S. law because of their cross-border operations, products, and ownership structures.

Software can be controlled under the EAR for many reasons, but by far the most common is for the use of encryption, which implicates Category 5 Part 2 of the Commerce Control List and the byzantine rules of License Exception ENC, 15 C.F.R. § 740.17. Depending upon the software's technical characteristics, the EAR may require a company to file with BIS a company encryption registration, a classification request, or to obtain an individual validated BIS licence prior to export. Even companies that provide open-source software may be subject to reporting obligations before making the software publicly available for download.

The OFAC regulations, which implement U.S. economic sanctions, claim jurisdiction over virtually all software exports or provision of SaaS from the United States. U.S. sanctions prohibit the export or supply of most software and services to comprehensively sanctioned countries and end-users. These prohibitions are in turn subject to various exemptions and general licences, including for facilitating personal Internet and other communications protected by the First Amendment.

Even companies that provide open-source software may be subject to reporting obligations before making the software publicly available for download.

At the risk of imperfect analogies, here are the 'seven deadly sins' of U.S. and non-U.S. software and SaaS companies that are regulated by BIS and OFAC.

1. PRIDE

Arrogantly assuming that your software is not regulated by U.S. law

This sin – the original and perhaps most deadly of the seven – is frequently committed by U.S. and non-U.S. companies alike.

Many U.S. companies wrongly assume that their software escapes regulation because of its seemingly benign nature and widespread availability. Why, they wonder, would U.S. national security depend upon where and to whom I distribute my business-focused, enterprise software? By our estimate, commission of this sin – or ignorance of the regulations altogether – gives rise to more violations of the EAR than all other sins combined. Despite several rounds of 'simplification' of the encryption rules, most software that performs, enables, or leverages encryption functionality continues to be regulated under the EAR. And because virtually all software fits this description, the default assumption should be that the software is regulated if it is made in or supplied from the United States, incorporates U.S.-origin content, or involves U.S.-origin technology.

Non-U.S. companies may also assume at their peril that their software is not regulated by U.S. law; and more frequently they fail even to consider it. A non-U.S. software or SaaS company may be subject to U.S. legal requirements where its software:

- although developed outside of the United States, is uploaded to a

server in the United States and made available for download from all locations (e.g., on the Apple iTunes App store or Android platform);
- is offered under a SaaS model and hosted from within the United States (e.g., U.S. servers maintained by Amazon Web Services), such that access from abroad is the exportation of a service from the United States;
- was developed using U.S.-origin technology or content; or
- is none of these things, but the non-U.S. company is sufficiently owned or controlled by U.S. persons – through a U.S. parent, U.S. investors, or a U.S. management team – that it is subject to U.S. sanctions against Cuba and Iran.

Failure to perceive these jurisdictional issues at an early stage means the resulting violations proliferate, often to be discovered at a critical juncture in the company's life cycle – e.g., in due diligence in connection with an investment, corporate acquisition, or initial public offering. Timing can turn an otherwise minor peccadillo into a sin of damning proportion, causing the investor or underwriter to insist upon a 'confessional' through voluntary self-disclosure of the violations to the relevant federal agency, or to withhold monies in escrow pending an agency resolution that might not occur for years.

The sin of pride is countered by a strong dose of humility and a rebuttable presumption that your product or service is regulated by U.S. law until a competent analysis proves otherwise.

2. WRATH

Allowing the complexity of U.S. export-control regulations to anger you to the point of neglecting a thorough compliance analysis

Even for those that manage to avoid the sin of pride, the complexity of the U.S. export controls and economic sanctions laws can frustrate software companies to the point of wrath. The virtue to counter wrath is a patient, thorough risk assessment leading to a proper jurisdictional conclusion and product classification – the keys to effective compliance. Under the EAR, 'classifying' the software involves reviewing the Commerce Control List ('CCL') to determine the software's Export Control Classification Number ('ECCN'), and then considering any licence exceptions that might apply to the software based on its technical characteristics.

While most software that is subject to the EAR is regulated as an 'encryption item' under Category 5, Part 2 of the CCL, do not forget that all ten categories of the Commerce Control List include software entries. A patient analysis considers whether other categories may apply before fixing narrowly on the EAR's encryption provisions.

Once you know how your software is subject to the EAR and classified on the CCL, you can determine your compliance obligations – e.g., whether company registration, reporting, or licences are required, and to which end-users and countries the software may be exported without a licence. This EAR classification in turn may unlock authorisations under U.S. economic and trade sanctions administered by OFAC.

If the jurisdictional or classification conclusions are incorrect, then the regulatory measures taken are also likely to fail, which can lead to export violations.

If the jurisdictional or classification conclusions are incorrect, then the regulatory measures taken are also likely to fail, which can lead to export violations. A company would be wise to make a formal BIS Classification Request wherever the classification of the product falls within a grey area, which is the case with many software products.

3. ENVY

Coveting another's favourable, open-source classifications and presuming that yours is entitled to the same

Some companies that have overcome pride and wrath still take risky shortcuts by assuming that their software merits the same regulatory treatment as a competitor's. But it is risky to covet another's export-control classification and treat it as your own. This is the sin of envy, and it is especially prevalent with open-source software classifications.

To qualify for an open-source licence exception in the EAR, a company must report to BIS the Internet location of its source code and provide it to the public 'for free or at a price that does not exceed the cost of reproduction and distribution'. (15 C.F.R. § 734.7(b) ('License Exception TSU')) Some companies do offer software in a free, open-source form via creative revenue models (such as advertisement-based, service add-on, or other 'freemium' models), but these remain the exception. To protect intellectual property, most companies export software in executable, compiled form.

Commonly, companies use open-source encryption APIs, libraries, or tools to develop proprietary software. This creates an entirely new encryption item that must independently satisfy the EAR's requirements. If the software is then distributed in executable form – i.e., the exported software is not source code made publicly available under the requirements of License Exception TSU – the TSU authorisation does not apply. And if it has not separately classified the software, possibly via a required classification request to BIS, violations ensue.

Similarly, under the OFAC regulations, source code may be exempt from regulation as 'information or informational materials,' whereas compiled software would not meet the terms of this exception. See, for example, Iranian Transactions and Sanctions Regulations, 31 C.F.R. §§ 560.210, 560.315, and 560.418.

Bertrand Russell once characterised envy as among the most prevalent causes of unhappiness. Had he been an export controls practitioner, he also might have seen envy as the source of unnecessary violations.

4. LUST

Providing a SaaS offering (because it's the sexy new thing

to do) without considering U.S. export control and sanctions laws

The SaaS model – including its variants, such as Infrastructure-as-a-Service and Platform-as-a-Service – seduces software companies to migrate their old-school, exportable software product into a SaaS offering. Even services such as Google Drive are taking the place of iconic, staple software installs such as Microsoft Word and Excel.

Under a SaaS model, the export-control considerations are fewer than for traditional exports of software. BIS does not regard the provision of SaaS to be an export of software, nor is the SaaS provider an 'exporter' of data transmitted from the cloud to locations outside the United States (although the user of the SaaS may be an exporter of data). But the compliance inquiry for a SaaS model cannot end there.

By providing access to a U.S.-based SaaS platform from outside the United States, the non-U.S. company thereby exports a service from the United States.

First, be sure to confirm whether any software is actually exported, or is instead fully accessible from outside the United States via open-source tools and software such as Internet browsers. If a SaaS offering uses downloadable client software (inclusive of plug-ins) for accessing the service, any 'exported' software invoking encryption functionality in the SaaS may pull the characteristics of the entire platform into the EAR. Likewise, many SaaS offerings are supported by mobile applications, offered on the iTunes or Android platforms, which are 'exported' when downloaded from outside the United States. On the other hand, if a SaaS platform merely exchanges data with a thin client through an open-source third-party tool (such as an Internet browser), this generally does not bring the SaaS platform within the EAR's jurisdiction.

Another 'watch out', even for pure SaaS companies, is that they may export their entire SaaS platform from the United States for hosting in another country, to minimise latency in the customer experience. Unless the source code is publicly available, the export of the platform is likely subject to the EAR. Although a licence exception authorises most such exports (see 15 C.F.R. § 740.17(a)), it is best to confirm. The nature of the service and customers should also be considered; although unlikely, these could implicate end-user and end-use prohibitions in the EAR, including for activities that 'support' missile and chemical/biological weapon proliferation.

An oft-overlooked wrinkle for non-U.S. companies is that by providing access to a U.S.-based SaaS platform from outside the United States, the non-U.S. company thereby exports a service from the United States. Accordingly, the foreign company sponsoring the U.S.-based SaaS is subject to the U.S. economic sanctions regulations, even if the non-U.S. company has no other connections to the United States. Without measures to shield access by persons located in comprehensively sanctioned countries or who are subject to OFAC sanctions, the SaaS provider invites significant risk. Time and again, non-U.S. SaaS providers select a U.S.-based cloud server (such as Amazon Web Service or Rackspace) and unwittingly bring themselves within the jurisdiction of the OFAC sanctions.

This focus on the OFAC sanctions brings us to our next deadly sin: Gluttony for customers.

5. GLUTTONY

Failing to screen customers against the sanctioned countries and denied-parties lists because of a hunger for any and all customers.

Compliance with U.S. law increasingly requires that you know some things about your customers. Gluttony is the sin of overindulging in customers without the necessary diligence.

OFAC sanctions generally bar exports from the United States or by a United States person to individuals and entities in comprehensively-sanctioned countries (Cuba, Iran, North Korea, Sudan, and Syria), and to persons and entities on OFAC's Specially Designated Nationals and Foreign Sanctions Evaders lists. For exports of software that is subject to the EAR, screening protocols should also include BIS's Denied Persons, Entity, and Unverified lists.

But knowing exactly how to navigate these list-based pitfalls is rarely obvious, and the options are many. Some companies screen customer names at sign-up ('dynamic' screening) to ensure that no country- or list-based rules are implicated. Others screen additional information – e.g., address, phone number, email address, or company website. Some companies, striving for a frictionless customer onboarding experience, defer the diligence and rely on periodic, batch screenings of existing customers, accepting the risk that a violation will have already occurred when it is identified. Other companies – particularly those not offering a free/trial version of their product – rely upon the screening efforts of financial service intermediaries (banks, credit card companies, et al.). Still other companies allow free-trial signups with nothing more than an email address, leaving little to be screened against a prohibited party list. Some seek compliance automation via IP-address blocking mechanisms, which are only partially effective against country-based sanctions violations. And many companies – the most gluttonous – gobble up customers with no attention to these risks.

Even well-intentioned companies find that none of these solutions is perfect. Screening generates 'hits' that must be investigated to determine whether they are true or false – a process that cannot be automated and requires human effort and judgement, taking time and risking alienation of the would-be customer. The IP-address blocking solution usually relies on third-party tools that present a high rate of false positives; unlike ordinary physical addresses, IP addresses are assigned to ISPs (which then re-assign the IP addresses to customers) and change over time, causing the tools to block even lawful customers. Many who live under repressive governmental regimes use proxy tools that spoof an IP address to bypass filtering mechanisms. Some companies wrongly assume that IP blocking is effective for compliance with list-based blocking requirements, unaware that the majority of OFAC Specially Designated Nationals are located in

countries that are not subject to U.S. sanctions. And the company that relies solely upon the screening conducted by a financial intermediary invites the risk that, once in receipt of OFAC-blocked payments, the intermediary may be obligated to report the matter to OFAC and expose the company to scrutiny.

Each of these approaches may be appropriate depending on the risk profile of the company adopting it. The key is to resist the sin of gluttony through a sensible diet tailored to your company's specific risk profile.

6. GREED

Falling victim to profit demands by continuing business as usual after discovering export-control violations

This deadly sin is often the most vexing and rears its head when a company is made to choose between compliance and profits.

Once a violation of the EAR is identified, General Prohibition Ten of the EAR provides that you may not 'sell, transfer, export, re-export, finance, order, buy, remove, conceal, store, use, loan, dispose of, transport, forward, or otherwise service, in whole or in part,' the unlawfully exported item. Yet that same item may be vital to your customer, who relies upon timely software updates or support that your company is suddenly and unexpectedly barred from providing. With contracts in place, and revenues at risk, the company facing a General Prohibition Ten issue is forced to face this 'sin against God,' which Thomas Aquinas described as 'condemn[ing] things eternal for the sake of temporal things'. Temptation beckons where the choice is between violating U.S. export-control laws or risking the loss of a significant customer relationship.

Often, the General Prohibition Ten conundrum is solved by filing a company registration or product classification with BIS, then exporting the now-lawful software to the customer, who is asked to replace the prior version with the lawful one – even if both versions of software are essentially the same. Recognising this may be form over substance, some choose to forgo the new export and deem the unlawfully exported software to be retroactively legitimised by the remedial filings. Construing the regulations to actually require the replacement of one thing with an identical copy, the argument goes, is nonsensical and contrary to the intent of the law.

Where these quick remedies are unworkable, the choices are fewer and the temptations greater. Some companies opt to quickly self-disclose the violations to the agency, continue servicing the unlawfully exported software, and simultaneously request expedited approval to do just that. But BIS is under no statutory timeline to respond to such a 'resumption of services' request – indeed, BIS may require a final voluntary self-disclosure before doing so. Meanwhile, the request itself may be considered an admission of intentional wrongdoing, at least theoretically exposing the company to criminal charges.

Under any scenario, be sure to address the collateral consequences of discovered violations and resist the sin of greed through careful weighing of the potential outcomes.

7. SLOTH

Taking initial steps to ensure compliance, but then lazily ignoring ongoing export control obligations

Here is a familiar narrative: A small software company starts to export products, not understanding how this is regulated. It later learns that its actions have led to possible violations, perhaps during diligence in connection with an investment. It goes to confessional by disclosing the violations to the relevant agency, and recommits to piety through a new compliance programme. The agency blesses the disclosure without issuing a penalty, and the company is spiritually cleansed and restored to what companies do best: developing and selling its product, full steam ahead.

Then comes the deadly sin of sloth – as 18th century philosopher Edmund Burke put it, the evil that exists 'when good men fail to act'. The antidote to sloth is diligence, and there are at least three important ways that every software company should exercise this virtue:

One, be sure to analyse changes to the software, which may require an updated encryption registration, classification request, or reporting. An obscure and frequently overlooked section of the EAR explains: 'A new product encryption classification request…or self-classification report… is required if a change is made to the cryptographic functionality (e.g., algorithms) or other technical characteristics affecting License Exception ENC eligibility (e.g., encrypted throughput) of the originally classified product.' (15 C.F.R. § 740.17(d)(iii)). Compliance here requires closing the gap between the software-development and legal/compliance functions within the company.

Two, be sure to analyse the technical characteristics of new products before release to see if any EAR filings are required. Similarly, consider whether OFAC regulations treat the software differently, e.g., because it has taken on a new ECCN that either qualifies or disqualifies the software under a general licence.

Three, remember that U.S. export control laws are dynamic and must be revisited periodically. As an example for this readership, software currently controlled as a 'cryptanalytic' item (15 C.F.R. § 740.17(b)(2)(ii)), or as a 'penetration testing' item (15 C.F.R. § 740.17(b)(2)(i)(F)), may face new EAR regulations after BIS implements the new 'intrusion software' category adopted by the Wassenaar Arrangement on Export Controls.

Diligence is the cure for sloth and should be inscribed in a sound, well-tailored compliance programme.

The way forward

To avoid eternal damnation via a denial of export privileges, crippling fines, or reputational damage, or even the purgatory of a lengthy agency investigation, software companies – U.S. and non-U.S. alike – should repent and get religion in the ways we have described in this article.

Rich Matheny is a partner and Jacob Osborn an associate at Goodwin Procter's Washington, DC office.

rmatheny@goodwinprocter.com

josborn@goodwinprocter.com