Recommendations for the Implementation of the 2013 Wassenaar Arrangement Changes Regarding "Intrusion Software" and "IP Network Communications Surveillance Systems"

Submitted by Access Now, Collin Anderson, Internews, Reporters Without Borders, and the New America Foundation's Open Technology Institute

May 5, 2014

Executive Summary

The uncontrolled export of surveillance technologies to countries with dubious human rights records poses a growing, significant threat to human rights and the free flow of information online. The authors of this document applaud the United States government for taking specific steps to address the spread of these technologies. These tools—commonly marketed directly to governments and designed to build surveillance and privacy-invasion capabilities into a country's communications infrastructure—pose serious threats not only to high-profile civil society and democratic efforts, but the daily lives of individual citizens at an unprecedented scale. With the recent export control amendments agreed upon at the multilateral Wassenaar Arrangement's December 2013 Plenary Meeting, this is a critical time for the United States to update export controls regulations to align with its well-defined human rights foreign policy objectives and to demonstrate international leadership on these issues. Integrating the proposed changes into the existing regime properly can reduce threats created by the uncontrolled trade of global surveillance while ensuring that general purpose computing and research are not affected. A targeted approach will also help avoid unintended chilling effects that could be created as a result of the new controls.

Given a diverse array of concerns and interests, we offer a number of considerations for drafting the controls, two proposals outlining options for specific control categories within U.S. export regulations, and several procedural recommendations.

Our recommendations can be summarized as follows:

- **Controls for surveillance technology must be implemented independent of encryption controls.** Focusing on the encryption capabilities of the technology in question would not only confuse two analytically distinct issues, but also fail to cover all of the relevant technology. Avoiding the application of encryption controls will help provide clarity, promote the further adoption of encryption online by minimizing regulatory complexity, and ensure compliance on both cryptography-related exports and for the proposed amendments. The development of distinct controls for surveillance technologies may also help prevent inappropriate reliance on encryption controls to reign in potentially harmful surveillance technologies, making it easier to ensure that controls are not overbroad.

- **The United States should carefully consider language and appropriate exemptions that capture the technology in question while minimizing risk to research and general purpose computing.** Protecting research and general purpose computing is critical to promoting Internet security, and new controls should be implemented in a manner that aligns with existing technology and software exemptions. We recommend that Wassenaar's "General Technology Note" and "General Software note under the Technology and Software – Unrestricted exemption" are replicated explicitly in American regulations for intrusion software.
- **Controls should include a case-by-case consideration for all destinations with a provisional presumption of denial.** The license consideration process for Intrusion Software and IP Network Communications Surveillance Systems must include examination of the human rights and privacy concerns that prompted their control, and exporters should have to prove that the goods or products in question do not pose a significant risk to human rights and national security. Because the proposed controls proposed describe surveillance technologies with limited legitimate applications, the determination process should provisionally maintain a general policy of denial for all end-uses and end-users for the two controls under consideration, recognizing that subsequent consultations with industry and civil society on performance and feedback are necessary.
- **Foreign availability provisions should not apply to control.** The transfer of surveillance technologies has a clear human rights impact with material foreign policy implications. Because there are significant potential negative effects from the uncontrolled export of such technology, the foreign availability provision should not apply to such technologies following existing precedent.
- **The technologies warrant new classification or application of strong existing controls**. General controls have not traditionally been applied for human rights purposes and are ill-equipped to cover the technology in question, so we recommend two options for how the Wassenaar amendments can be integrated into the U.S. export control regime:
    - **Preferred option:** Expand the definition and current application of existing Surreptious Listening (SL) controls, or create a replacement control (e.g.

"Surveillance Technology" control) that covers the broad range of the communication intercepting devices, from mobile interception equipment to intrusion software.

  - **Alternate option:** Implement controls through the Crime Control list, which contains a relevant control that parallels the need for both strict regulatory oversight and consideration of human rights implications.

- **Once implemented, the effectiveness of the control relies on more active U.S. government involvement before and after export**. Non-compliance will be a major issue, and effective controls on intrusion software and network surveillance equipment will require clear "know your customer" policies and aftermarket verification. We recommend that federal agencies offer specific "know your customer" guidance and red flags, require sales material and documentation of policies as part of license processes, and institute policies that create strong deterrent effects for the export of these technologies.
- **Export control processes related to surveillance technology should promote transparency and participation from civil society and industry.** Export control agencies should provide greater public data on the implementation and enforcement of the proposed and existing controls on surveillance equipment. Industry and civil society also need to be included in the process to ensure that federal agencies' efforts match the fast pace of technological development.

I. Introduction

The uncontrolled trade of surveillance technologies to countries with dubious human rights records poses a growing, significant threat to human rights and the free flow of information online. We applaud the United States government for its leadership in updating sanctions regimes to specifically address the spread of these technologies, as well as its demonstrated interest in utilizing export control regulations to do the same on a broader scale. We believe these tools—commonly marketed directly to governments and designed to build surveillance and privacy-invasion capabilities into a country's communications infrastructure—pose serious threats not only to high-profile civil society and democratic efforts, but also to the daily lives of entire populations.

The "sensitive technology" definitions provided by the State Department last year in response to the Iran Threat Reduction and Syria Human Rights Act[1] were an important first step in defining technologies that warrant additional scrutiny. The language signaled that the United States seeks to address reports that American-made network equipment has been directly instrumental to the violation of human rights in repressive countries. In the past few years, ample evidence has been uncovered that such hardware and software is used not only to violate internationally-recognized civil and political rights in sanctioned countries, but also globally. In particular, their use has been documented in non-sanctioned countries whose systematic persecution of dissident and minority groups has been demonstrably aided by sophisticated communications-monitoring equipment. Meanwhile, because of the widespread availability of these technologies, businesses and nongovernmental organizations in the United States are increasingly subject to industrial and political espionage by foreign governments and companies seeking to steal trade secrets. For these reasons, this is a critical time for the United States to update export controls regulations to align these policies with its well-defined human rights foreign policy objectives.

The recent export control amendments agreed upon at the multilateral Wassenaar Arrangement's December 2013 Plenary Meeting also present an opportunity for the U.S. government to reassert an international leadership role on matters of Internet Freedom.

[1] See also "Comments Regarding Sensitive Technologies Guidance" submitted to the U.S. Department of State in January 2013 on behalf of many signatories to this comment, http://oti.newamerica.net/publications/resources/2013/comments_regarding_sensitive_technologies_guidance.

Integrating the proposed changes into the existing regime properly can reduce threats created by the uncontrolled trade of global surveillance while ensuring that general purpose computing and research are not affected and promoting the adoption of norms internationally that address concerns over foreign availability. In the past, the U.S. government has usually incorporated Wassenaar changes into its national export control regime faster than other member states. As a result, the manner in which the United States implements these changes typically offers a blueprint for other countries to follow and build on.

At the same time, we recognize the lessons learned from previous efforts to use export controls as a means of regulating information technologies, particularly those containing encryption—namely the risks of inadvertently inhibiting academic and commercial work on information security. Thus, it is essential that these changes are also implemented with clear exemptions and guidance to the public so that the controls are not interpreted in an overbroad manner. A targeted approach will also help avoid unintended chilling effects that could be created as a result of the new controls.

Given these diverse concerns, we offer the following recommendations based on our assessment of the technical and administrative challenges. These recommendations are guided by civil-society perspectives, including examples where the export of surveillance technologies led to direct harms. We outline general considerations that we believe should be incorporated into the implementation of the new controls, as well as specific recommendations of how to integrate the new controls in the existing regime. We argue that federal agencies have a substantial role in performing active due diligence on the export of technologies that have serious human rights applications, and that they must establish strict requirements on the transfer of this technology to all destinations. Together, these proposals aim to create an effective export control regime and template for other countries to build on.

II. Controls for Surveillance Technology Should Be Implemented Independent of Existing Encryption Controls

As reflected in the Wassenaar changes, which incorporated the additions of "intrusion software" and "IP network communications surveillance systems" in categories 4 (Computers) and 5 Part 1 (Telecommunications), respectively, rather than category 5 Part 2 (Information Security), implementation of the proposed changes in the US regulatory framework should not reference or rely on encryption controls. Such equipment and software may include encryption as a component of its operations, but these functions do not by definition require encryption, so a control that focuses on cryptography would not achieve the objectives of the Wassenaar additions. In the past, BIS has issued encryption exemptions to promote Internet security, and we expect that the future of encryption controls will be further debated in light of renewed public focus on communications privacy and its role in modern electronic commerce. Combining cryptographic controls with this new area of surveillance technologies would make it more difficult to address and revisit the two distinct issues going forward. Consequently, such a classification would run contrary to the very essence of the proposed controls.

This analysis is based on three findings:

1. **Encryption controls are an analytically distinct (and highly debated) issue.** Since License Exception TSU was issued, encryption controls have been the subject of public debate and eased within the past decade in order to promote commercial and personal use of tools that use encryption. The Wassenaar amendments fit within the framework of liberalizing controls further, addressing widespread concerns over information security in the digital age. Therefore, tying encryption controls to surveillance technology would potentially undermine the objective of both efforts, particularly given that encryption technology is not the primary use or concern that led to regulations on intrusion software and network surveillance equipment.
2. **Encryption controls would not cover all relevant technology.** While the use of encryption is commonplace in surveillance and intrusion technologies, encryption is not always necessary to their core functionality and could even be removed by vendors seeking to avoid export controls. In one case, the UK government used encryption controls in order to limit the export of Gamma International Ltd's FinFisher intrusion

software to foreign governments. However, this approach potentially makes it possible for companies such as Gamma to avoid such controls by changing their product's encryption key length or end destination,[2] or simply by removing encryption altogether.

3. **Existing mechanisms to streamline encryption export are not appropriate for surveillance technologies.** Significant progress has been made to simplify licensing procedures for encryption products, which is a positive development given the increasing use of encryption technology in a wide variety of products and its role in protecting privacy online. For example, license exceptions and registration/self-classification procedures permit certain exports of encryption products without a license. Unlike most encryption items, however, surveillance technologies present such a significant risk to human rights that License Exception ENC is in certain respects incompatible with effective implementation of the Wassenaar changes. Overlap exists between the items designated under §740.17(b)(2)(i)(F) of the license exception and the new Wassenaar controls related to "intrusion software," creating a potential conflict in application. Under §740.17(b)(2)(i)(F), companies are permitted to engage in simplified classification review and export of "encryption commodities and software that provide penetration capabilities that are capable of attacking, denying, disrupting or otherwise impairing the use of cyber infrastructure or networks," if the export is not to a "government end-user." This may include telecommunications companies, Internet service providers and educational organizations—entities that in many countries are in fact controlled by, or substantially beholden to, governments and other local authorities.[3] In any event, the language would apply to some surveillance technologies that would also fall under the definition of "intrusion software," and so may require modification. The end control applied to the Wassenaar changes should grant export control organizations stronger discretion in the future over the exportation of these technologies than is currently mandated under License Exception ENC.

[2] End destination can be defined as not only the country, but also the person or entity within a country. For example, encryption controls have favorable considerations or do not require licenses for particular locations or end users. This makes it easier to sell to a private company (including ones that may be contracted by a government) than a government itself.

[3] Given the offensive capabilities and potential human rights implications of such technology, it is unclear why the license exception covers items with such "penetration capabilities" in the first instance, rather than excluding those items entirely from the scope of the exception, and requiring a complete license application for case-by-case review of such exports to all end-users

For these reasons, we believe that avoiding the application of encryption controls will help provide clarity, promote the further adoption of encryption online by minimizing regulatory complexity, and ensure compliance on both cryptography-related exports and for the proposed amendments. Furthermore, the development of distinct controls for surveillance technologies may help prevent inappropriate reliance on encryption controls to reign in potentially harmful surveillance technologies, making it easier to ensure that controls are not overbroad. This would align with the intent and objectives of the Wassenaar proposals, as well as maintain a high standard for surveillance technology in the medium to long-term.

III. Existing Wassenaar Definitions and Exemptions Provide a Framework for Implementation

Upon publication of the Wassenaar proposals, concern was expressed[4] about whether the intrusion software language could be applied to common, off-the-shelf security applications and 'jailbreak' tools (software that allows a user to circumvent manufacturer protections in order to modify their own device). In contrast to the technical specificity of IP network surveillance, the controls outlined for intrusion software could potentially be interpreted broadly (based on the export control agency discretion) to include more than commercial surveillance technologies. Intrusion controls should not threaten the public's ability to control personal devices or prevent researchers from engaging in security auditing, even where it may include the discovery of vulnerabilities. While we express later our concerns about the potential of 'specially-designed' and 'quality of service' exemptions to be misused, it is equally important to remember that overbroad language could intentionally or inadvertently be used to stifle jailbreaking, security research, and additional activities that would otherwise promote privacy or general purpose computing. We urge BIS to define intrusion software narrowly to cover non-consensual, second-party surveillance, and to provide exemptions or clarifications in order to protect against overly broad interpretations. BIS advice should include an explanation to the "fundamental research" deemed export exemption to clarify that independent security researchers working outside a traditional academic context (for instance, volunteers, or involved in co-operation between commercial and non-commercial groups) can be exempted for work whose purpose is to document or mitigate surveillance and intrusion attacks against end-users.

The current language under Wassenaar's General Technology Note and General Software Note provides a framework for guidance that should be replicated within American regulations governing these technologies. Therefore, we support exemptions for technologies that are of the same spirit as the Technology and Software – Unrestricted (TSU) exemption. Effective exemptions would cover open source technology and activity by the legitimate academic and security community. If exemptions are too loose, they present a loophole and risk of reclassification of control.

[4] Jennifer Granick and Mailyn Fidler, "Changes to Export Control Arrangement Apply to Computer Exploits and More," Just Security, January 15, 2014, http://justsecurity.org/2014/01/15/export-control-arrangement-apply-computer-exploits/.

The proposed technical definition of IP Network Communications Surveillance Systems includes a note that exempts systems or equipment specially designed for marketing, network Quality of Service (QoS), or Quality of Experience (QoE) purposes. However, while these exemptions exist for the commendable purpose of mitigating potentially overbroad regulation of ordinary network technologies, they also create significant risk for the misclassification or re-appropriation of equipment that bear the same capacity for material harm as those specifically branded for surveillance purposes. The language of the provision lists five qualifying characteristics (six when including ‘carrier class’ wording) outlined in order to limit the forms of equipment controlled. This creates an extremely narrow definition that illustrates a special class of technology, one which far exceeds normal consumer products and reduces the potential technologies down to a manageable set for which a license and due diligence should be required. However, the technical nature of the control is challenged by the flexibility of the language of the note. QoS and QoE are broadly-defined functions that have often been appropriated for the disruption or monitoring of the free flow of information around the world. Reliance on these ambiguous terms means that the "dual use" nature of any particular technology may be used as grounds to exclude it from control. The EAR language must take into consideration this potential weakness of the exemption note, and the threat posed by these technologies regardless of their advertised purpose. At a minimum, BIS should provide clear guidance on the intention and limitations of the technical terms used within the control's note in order to more thoroughly clarify its applicability and minimize potential misclassification.

IV. Considerations for Constructing New Controls: Licensing and Review Process, Qualifications, and Foreign Availability Provisions

The technologies adopted by the Wassenaar plenary pose significant dangers when provided to governments and non-state actors in countries that fail to respect internationally-recognized human rights norms or who present national security concerns. While components of existing controls offer opportunities to address certain considerations, they do not discretely or congruently fall into an existing framework. The current situation reflects not only the growing norm of controlling the provision of surveillance technologies, but also concerns about legitimate commercial interests. In one case, discussed in depth later, relevant surveillance technology for the interception of mobile communications appears to have been previously classified under a National Security (NS) control. While the imposition any control at that time was a positive step, the decision also created incongruities with respect to the regulation of similar technologies. Moreover, it failed to take into account the full need for strong due diligence.

General control regimes, such as Significant Items (SI), National Security, Regional Stability (RS), and Anti-terrorism (AT) define licensing requirements and presumptions of acceptance within regions that may not be appropriate for surveillance items. These classifications have not historically been applied for human rights purposes, and thus the procedural considerations invoked, inter alia, are not demonstrably equipped to handle critical contingencies or consult with all relevant entities. Furthermore, limited oversight based on Country Groups places export control agencies in the position of publicly outlining "acceptable" countries, a process subject to external political pressure that would dilute its effectiveness, These concerns are reinforced because of recurring cases of transshipment of such technologies through third-party countries.

The classification applied and its enforcement by federal agencies should be tailored to specifically address the challenges presented by:

1) the nature of the technologies,
2) the reasons for implementing controls,
3) the pertinence of existing Export Control Classification Numbers (ECCNs), and
4) the possibility for further expansions to the list of items.

Therefore, we outline specific requirements for efficient oversight that should be implemented regardless of the end classification, and then propose two potential means of control in order to

achieve the Wassenaar amendment objectives in a uniform manner.

<u>Consideration</u>: Control Should Include a Case-by-Case Consideration for All Destinations with a Provisional Presumption of Denial.

The license consideration process for Intrusion Software and IP Network Communications Surveillance Systems must include examination of the human rights and privacy concerns that prompted their control. In order to ensure that these are central to the review process, the applied control must put the onus on the prospective exporter to prove that the goods or products in question does not pose a significant risk to human rights and national security before the licensing decision. We maintain concerns about the potential chilling effect of overbreadth on the development and international availability of technologies necessary for modern telecommunications infrastructure in cases where network and computing equipment are administered under broadly-defined export controls or have legitimate dual-use purposes. However, the controls proposed in December 2013 describe surveillance technologies with limited legitimate applications. With the incorporation of Wassenaar's General Notes and consideration of additional recommendations outlined herein, we believe that the proposed language and technical definitions are narrowly-tailored and appropriate to the small set of technologies of concern. Therefore, the determination process should provisionally maintain a general policy of denial for all end-uses and end-users for the two technologies under consideration, recognizing that subsequent consultations with industry and civil society on performance and feedback are necessary. A presumption of denial for these technologies may also be instituted with the understanding that any future controls imposed on other surveillance technologies could require more flexibility and discretion. If appropriate in the future, we would encourage export control organizations to balance varying levels of risk by creating separate sub-control codes that would allow for more favorable processes or destination-based exemptions, similar to existing variations in country charts and ECCNs.

The work of research organizations like the Citizen Lab has demonstrated that the most active customer bases for the technologies described by the 2013 Wassenaar amendments are often in countries that lack adherence to rule of law and ignore internationally-recognized human rights, including freedoms of association, expression, religion and privacy. However, because these technologies call attention to the decreasing cost and increasing efficiency of mass

surveillance on entire populations,[5] we caution against a favorable licensing policy to any destination. Even within democratic societies that have robust rule of law and civil liberties protections, the use of such technologies by law enforcement and intelligence agencies has been called into question. A one-time lapse in export controls can be all it takes for a repressive government to acquire the technological components central to broad national surveillance programs. Therefore, effective enforcement requires case-by-case consideration of licenses for all countries, and should refrain from destination-based exemptions even for close allies or otherwise stable export control regimes.

Historical cases of the transshipment of surveillance technologies through third-parties demonstrate the limited effectiveness of reliance on prohibitions based on regimes such as Country Groups D and E. Countries that fall with Group B, potentially subject to License Exception GBS for items under National Security controls, have also been used to reroute technologies subject to sanctions restrictions by the United States and other governments. In the absence of outside licensing oversight, sanctions regulations were unable to stop an intermediary in Denmark from rerouting NetEnforcer Deep Packet Inspection equipment manufactured by the Israeli firm Allot Communications to Iran, despite indications that the purchaser was engaged in questionable behavior.[6] In another case, the SEC expressed concerns that resellers made Hewlett Packard Co. systems available to an Italian company, Area SpA, as a component of Syria's nationwide surveillance and tracking system.[7] Furthermore, transnational telecommunications firms, often headquartered in European or other allied countries, are frequently required by local laws governing their international subsidiaries to directly provide lawful interception equipment. Given the expansion of European telecommunications companies into at-risk environments, such as Norway's Telenor in Myanmar, it's clear that exports to stable environments may end up in another country's network. These lawful interception mandates imposed by foreign governments that international telecommunications firms operate within have already played a role in the

[5] Kevin S. Bankston and Ashkan Soltani, "Tiny Constables and the Cost of Surveillance: Making Cents Out of *United States v. Jones*," *The Yale Law Journal*, January 9, 2014, http://yalelawjournal.org/forum/tiny-constables-and-the-cost-of-surveillance-making-cents-out-of-united-states-v-jones.

[6] Ben Elgin, "Israel Didn't Know High-Tech Gear Was Sent to Iran," *Bloomberg News*, December 23, 2011, http://www.bloomberg.com/news/2011-12-23/israel-didn-t-know-high-tech-gear-was-sent-to-iran-via-denmark.html.

[7] Nicola Leske, "HP says products may have been sold to Syria by others," *Reuters*, November 23, 2012, http://www.reuters.com/article/2012/11/23/us-hp-syria-idUSBRE8AM0U920121123.

acquisition of surveillance equipment by the Iranian government, as alleged in the provision of American systems to MTN Irancell through South African firm MTN.[8]

<u>Consideration:</u> Licensing Process Should Take Into Account Existing Human Rights Practices and Expertise Within Government.

We recommend mandatory and strong consideration of human rights in the process of making decisions on specific licenses for all end destinations, particularly given the documented ease with which law enforcement functions can turn into the repression of religious, political, and ethnic minorities. Engagements on the promotion of religious freedom and Internet freedom through the State Department and Congress have created vast institutional knowledge inside government on the context of potential transfers, which as we note bear consideration given how these technologies can potentially be used to conduct absolute surveillance on entire populations. The documented sales claims of companies providing technologies that would fall under the proposed control, including from American vendors, reinforces reality of these dangers, offering to "monitor a hundred thousand targets"[9] and to "see what they see, in real time."[10]

The United States has established a rich set of considerations and processes applied to the Crime Control (CC) list, including provisions of the International Religious Freedom Act of 1998 (IRFA), the Department of State's Human Rights Reports and Leahy Law. As a result, the United States imposes limitations on the availability of crime control items to governments found to engage in violations of human rights. Regardless of classification, the precedent and consultative structure established for the CC list must apply to the forthcoming control.

Federal agencies must ensure that the United States does not facilitate the transfer of surveillance technologies to countries that violate human rights, promote regional destabilization, or bear transshipment risk. The control process should also include mandatory consultation with human rights entities within and associated with the United States government, such as the State Department's Bureau of Democracy, Human Rights and Labor, the United States Commission on International Religious Freedom and relevant Internet Freedom programs, on each application for each destination. In cases where these entities experience capacity gaps, we strongly

[8] Steve Stecklow, "Special Report: How foreign firms tried to sell spy gear to Iran," *Reuters*, December 5, 2012, http://www.reuters.com/article/2012/12/05/us-huawei-iran-idUSBRE8B409820121205.
[9] Hacking Team, "Remote Control System: Cyber intelligence made easy," https://www.documentcloud.org/documents/409278-147-hackingteam-rcs.html.
[10] SS8, "Intellego," http://www.ss8.com/sites/default/files/SS8_Intellego_Brochure.pdf.

recommend increasing resources to ensure efficacious consideration.

In the absence of structural requirements for consultation, we are concerned that the current process in place and the composition of the inter-agency group are not designed to take human rights considerations sufficiently into account, and may lead to the mistaken provision of sensitive technologies to bad actors in a manner that is contrary to a human rights-informed foreign policy.

Consideration: Controls Should Clarify "Specially Designed" Qualifications without Overreaching.

The implementation of controls for both intrusion software and network surveillance equipment must clarify, and where possible, avoid intent-based parameters for surveillance items, particularly given the danger of misclassification under more permissive ECCNs through rebranding. It remains unclear, for example, whether export control organizations considered devices capable of extensive Internet monitoring and censorship as "specially-designed" communications intercepting devices under Surreptitious Listening controls. As a result, the existing regulations have created unclear and incongruent compliance regimes, with accusations of cheating.[11]

Ongoing research on international surveillance systems has demonstrated a consistent transfer of sophisticated surveillance technologies from the United States under the auspices of normal network management. The key obstacle is that many surveillance technologies can have both legitimate and illegitimate uses under international human rights standards. Nevertheless, recent trends demonstrate that export control organizations need to not only perform significant due diligence on the end use and user of the transfer, but also provide clear guidance regarding such definitions. We are concerned that regulating only technologies that advertise themselves explicitly as surveillance equipment would continue to make it possible for dangerous goods to be provided under more permissive rules. The final rules for both proposals should address technologies where the properties of the product may permit it to potentially achieve or exceed stated performance levels, characteristics, or functionality in order to conduct intrusion or surveillance functionalities.

[11] *Glenford J. Myers v. IP Fabrics*, Inc., http://media.oregonlive.com/siliconforest/other/IPnFabrics.pdf.

<u>Consideration</u>: Foreign Availability Provisions Should Not Apply to Control.

Regardless of whether it is controlled through the Crime Control list or an expansive Surreptitious Listening classification, the transfer of surveillance technologies has a clear human rights impact with material foreign policy implications. Because there are significant potential negative effects from the uncontrolled export of such technology, the foreign availability provision should not apply to such technologies. The new control can bolster the United States' agenda of promoting access to communications and move beyond rhetoric.[12] Moreover, while international vendors may offer products that purport to compete on a like-for-like basis with American and European companies, communications interception infrastructure differ meaningfully from items such as thumbscrews or other instruments of torture. The entities providing such equipment from the West produce cutting edge technologies that often exceed their competition in sophistication and after-market service. For example, while the development of basic Internet censorship infrastructure is relatively unsophisticated and may not require outside assistance, the installation of scalable and responsive filtering apparatuses requires more resources. Foreign countries import such equipment for the service and support provided, such as backend systems from the vendor that are capable of using artificial intelligence algorithms to automatically to determine whether a previously unknown website should be blocked. Both the CC and SL currently maintain that despite foreign availability, such regulation is critical because it minimizes the risk of provision to illegitimate actors and serves American foreign policy interests.

[12] The technologies defined for control are directly antagonistic to those developed through funds provided by the Department of State and Broadcasting Board of Governors: http://www.state.gov/e/eb/cip/netfreedom/index.htm.

IV. Specific Recommendations for Controlling Surveillance Technologies through a New Classification or Application of Strong Existing Controls

Below, we outline two possible options for incorporating the IP Network Surveillance and Intrusion Software technologies into the existing U.S. export control regime. We recommend that strong consideration be given to the preferred option, which is to create a new "Surveillance Technology" (ST) control or revise and expand the existing Surreptitious Listening (SL) control to cover the relevant technology. We believe that this is the clearest and most logical path for the U.S. government to take to incorporate surveillance technology in a way that best captures the characteristics and specific risks presented by this technology. Our alternate recommendation would be to integrate the Wassenaar amendments into the Crime Control list.

Preferred Option: *Create a New "Surveillance Technology" Control, or Revise and Expand the "Surreptitious Listening" Control.*

The United States should either expand the definition and current application of existing Surreptious Listening (SL) controls, or create a replacement control (e.g. "Surveillance Technology" control) that covers the broad range of the communication intercepting devices, from mobile interception equipment to intrusion software. On its face, the definition of communication intercepting devices in the existing SL control applies to both proposals under consideration from the Wassenaar plenary. Both intrusion software and network surveillance equipment fall under the established description of "electronic, mechanical, or other devices that can be used for interception of wire, oral, or electronic communications if their design renders them primarily useful for surreptitious listening even though they may also have innocent uses" (15 CFR 742.13). Moreover, the existing requirement for licenses aligns with the considerations outlined above. However, questions remain about the uniform interpretation and application of these controls on digital surveillance technologies, as well as how other Wassenaar member states would follow the example of a previously unilateral control.

The type of technology and reason for control within the category of communications interception devices are so specific that they require a stand-alone and coherent definition, licensing policy, and enforcement mechanism in order to remain both up-to-date and effective. By creating such a control, export control agencies would be able to better address prior aversions to the control of digital communications equipment that arise from the rapid growth of

technology. This would also facilitate the issuance of a license exception under the new control in order to ensure that it does not chill research, privacy, and security work. Finally, most existing controls, particular NS, were neither designed for this new problem nor have a specific focus on human rights, one of the key reasons for and elements of the new controls.

Within existing ECCNs in the Commerce Control List (CCL), several technologies are relevant in the context of surveillance technology, namely those defined under 5A980 as devices primarily useful for the surreptitious interception of wire, oral, or electronic communications. More tangibly, ECCN 5A001.f outlines "mobile telecommunications interception or jamming equipment, and monitoring equipment," which are both pertinent to the present concerns and inconsistently controlled. Section (f.1) defines "interception equipment designed for the extraction of voice or data, transmitted over the air interface" as *Surreptitious Listening*, whereas the following control on equipment "designed for the extraction of client device or subscriber identifiers (e.g., IMSI, TIMSI or IMEI), signaling, or other metadata transmitted over the air interface" is subject to *NS Column 2*. Finally, jamming equipment designed to "intentionally and selectively interfere with, deny, inhibit, degrade or seduce mobile telecommunication services" falls under *NS Column 1*. It is unclear whether distinctions exist due to historical circumstances in their implementation, the fact that the controls were added at different times, or a narrow interpretation by BIS of the definition of communications interception. However, all three controls clearly define similar instances of monitoring and disruption of communications technologies that warrant congruent consideration processes and conditions for export.

The control of surveillance, law enforcement and intelligence gathering tools should be uniform and comprehensive. Piecemeal approaches such as that of 5A001.f, or separating existing items from the proposed rules, render control initiatives ineffective for industry compliance and civil society accountability strategies.

<u>Alternate Option:</u> Application of the Crime Control Classification.

Alternatively, the Crime Control (CC) list contains a relevant control that parallels the need for both strict regulatory oversight and consideration of human rights implications. Furthermore, recent additions to the list are related to identification and tracking technologies, such as automated fingerprint and identification retrieval systems, psychological stress analysis equipment, electronic monitoring restraint devices, and voice print analysis equipment. The CC

classification closely aligns with the objectives of the control to mitigate the human rights risks that are prevalent in their exportation. The incorporation of the International Religious Freedom Act of 1998 (IRFA) and Department of State's Reports on Human Rights Practices creates the policy of denial for license applications to export crime control items to countries whose government has engaged in gross violation of human rights that is appropriate for these technologies. Application of any classification other than CC must include parallel due diligence provisions.

V. Considerations to Ensure that Controls are Effective: Know Your Customer Guidance, Documentation, and Deterrent Effects

Within the short history of the commercial market for Internet communications interception technologies, there are a litany of examples of equipment being transshipped to sanctioned countries through intermediaries and out-of-compliance vendors. Effective controls on intrusion software and network surveillance equipment will require clear "know your customer" policies and aftermarket verification. Export control agencies have a responsibility and opportunity to define compliance with the guidance that they offer to vendors and the material required for approval.

Consideration: Federal Agencies Should Offer Specific Know Your Customer Guidance and Red Flags.

Digital surveillance technologies provide opportunities for post-shipment verification that most controlled items do not, which should be incorporated into the guidance provided by U.S. regulators. The enforcement actions by the Department of Commerce's Bureau of Industry and Security against Waseem Jawad, Computerlinks FZCO and Infotec exemplify the opportunities for post-shipment compliance within the proposed set of technologies. Mr. Jawad was found to have ordered multiple Blue Coat proxy devices from an authorized distributor in the United Arab Emirates with the false destination of Iraq's Ministry of Communication. Instead, these devices were transferred to the Syrian Telecommunications Establishment to be used as a core component of the regime's surveillance and censorship apparatus. Upon the public disclosure of these devices, a Blue Coat spokesman stated that "we see no firm evidence that would determine there is Blue Coat equipment in Syria; in fact, it appears that these logs came from an appliance in a country where there are no trade restrictions." However, the documentation and log files released from the Syrian devices demonstrated that the devices made calls back to Blue Coat to update its censorship database and retrieve software updates, revealing its true location.[13]

Federal agencies should both assist in the development of and mandate "know your customer" policies on the identification of potential clients and monitoring of behavior, based on red flags that could indicate a potentially suspicious transaction. The Commerce Department has

[13] Collin David Anderson, "BlueCoat and Syria: Indicators and Culpability," October 11, 2011, http://b.averysmallbird.com/entries/bluecoat-and-syria-indicators-and-culpability.

previously developed lists of such red flags for general purposes, as well as for specific sectors. These lists do not need to be all-inclusive, but would be intended to illustrate the types of circumstances that should cause reasonable suspicion that a transaction will violate the EAR, and instruct future investigations of breaches. Such due diligence should explicitly include after-sales knowledge and remediation, given that both hardware and software, as part of its normal maintenance, diagnostic reporting, or update cycles, may communicate with its original manufacturer. Furthermore, documentation, software and firmware updates may also be proactively downloaded by customers, creating more indications of the location or usage patterns of such technology. Absent such mandates, there is a risk that individuals or entities may "self-blind" by ignoring the location or the uses reflected by such requests, necessitating BIS's upfront involvement in defining minimum standards. Additionally, it should be emphasized, especially in light of the Syrian case, that within the guidance, "know your customer" encompasses "know your reseller" and "know your regional partners" – in short, "know your end user". Regional entities and third-parties may be unaware of the liabilities that the original vendor would incur and legal responsibilities that they retain. These may also include human rights impact assessments in regions where the risk to free expression and privacy is at its greatest, similar to those proposed by the Global Network Initiative and Electronic Frontier Foundation.[14]

Pertinent red flags may include:

- Originating IP addresses and network information for software updates and other device-related communications;
- Customer registration information;
- Stated end use by the customer and placement of technology within the network;
- Technical discussions or questions from potential customers;
- Requests for customization.

Finally, recurring outreach to industry and civil society should be conducted in order to ensure that export control agencies' guidance matches not only the fast pace of the technological development, but also changes in the ways infringing parties may attempt to bypass controls. This outreach may also expose cases where regulation may be overburdensome on the provision of non-surveillance network functionalities and therefore needs to be refined. More broadly,

[14] *See*, e.g., Cindy Cohn, Trevor Timm, and Jillian C. York, "Human Rights and Technology Sales: How Corporations Can Avoid Assisting Repressive Regimes," Electronic Frontier Foundation, April 2012, https://www.eff.org/document/human-rights-and-technology-sales.

these engagements should coordinate the sharing of expertise and experiences, mitigating potential information gaps in enforcement, and improving the role of civil society initiatives, such as the public "know your customer" frameworks developed by technological organizations.

<u>Consideration</u>: License Processes Should Require Sales Material and Documentation of Policies.

Considering the breadth of both legitimate and illegitimate use cases for surveillance technologies, export control organizations should avoid deploying purely a "bright line" test on review, and instead require thorough documentation from vendors on each transfer before approval. Such an approach would accommodate differences in circumstances of deployment and detect attempts to mischaracterize transfers.

For example, after the Blue Coat network appliances were found to be used for censorship in Syria, the company noted that their devices were not designed for surveillance purposes. As with any network caching device, such equipment is capable of both legitimate, modern network functionalities such as blocking malware and reducing load, as well as potentially illegitimate activities such as logging user traffic and filtering political content. Similarly, deep packet inspection has an established utility in ensuring the information security of businesses and protecting users. However, approved application of the technology can be differentiated from potentially infringing situations based on the user, use case and operational details of the attempted export. Special attention should be paid to ensure that vendors of sensitive technologies cannot bypass export regulations by slightly modifying means, approach, or branding.

These dual use scenarios warrant significant review from export control organizations on contractual documentation, and can be achieved without introducing rigidity that stifles enforcement or overburdens vendors. Such documentation may include, but not be limited to:

- Relationship with the contracting entity, including length of relationship, contractual mechanisms for compliance and demonstrated reliability (with respect to both export controls and sanctions);
- Final country destination, recipient, and end use of the technology, such as location in a network or nature of the buyer, supported by clear and detailed documentation;
- Extent of ongoing servicing of the technology, including potential for post-export checks on compliance;
- Design of the technology and customizations.

<u>Consideration</u>: New Precedents Require Strong Deterrent Effects.

The nature of the technology outlined within the 2013 Plenary Amendments is increasingly intangible and therefore subject to greater transshipment risk. Proper control of the transfer of these potentially virtual items requires both strong guidance from export control organizations, as well punitive mechanisms for when violations occur. This will create a deterrent to increase the regime's overall effectiveness.

As with the case of Blue Coat equipment in Syria, the uncontrolled release of surveillance technologies bear risks that vastly exceed the products' monetary value, These concerns are potentially more pressing with regard to software that may be copied and redistributed,. Once shipped, technologies that end up in the hands of malicious actors can no longer be controlled and remain a permanent part of the surveillance or espionage infrastructure of repressive states and non-state actors. The use of deemed export rules will be increasingly central for policing the transfer of virtual goods, where functionalities and infrastructure may remain housed in the United States and still used to conduct surveillance on at the behest or control of foreign parties.

In addition to guidance on the role of deemed export rules from the outset, penalties must therefore be used for deterrent purposes, in order to encourage responsible compliance and due diligence processes rather than simply to seek remuneration for damages. Export enforcement agencies must have the means and be encouraged to pursue criminal and administrative penalties to the fullest extent available for infringing activity that does not qualify under research exemptions. In light of the seriousness of these concerns, penalties should not only be limited to monetary repercussions based on the value of the item, but must also include consideration of denial of export privileges, potential imprisonment, property seizure and the fullest financial penalties available.

VI. Procedural Recommendations and Conclusion

Finally, we believe that the utilization of reporting and consultation mechanisms that exist within other areas of the American export control regimes will increase transparency and efficiency, both inside and outside of government. **Export control organizations should provide greater public data on the implementation and enforcement of the proposed and existing controls on surveillance equipment**. This is crucial in order to make the information required to assess the effectiveness and utility of the various controls available. Better public information also enables companies and non-governmental organizations to gain a better understanding of existing practices, to facilitate accountability by encouraging multi-stakeholder cooperation on due diligence principles, and to better inform the implementation of such regulations.

Taking into account notification requirements from the Wassenaar Arrangement's Sensitive and Very Sensitive Lists, **the form of such disclosure may include information outlining the following**:

- Number of license applications overall, listed by ECCNs and end destination, including the number successful and rejected applications, disaggregated;
- Details for denied applications, including:
    - Country exported involved in the transfer and stated end destination;
    - Item number on the Control List;
    - Short description, stated end-use and other relevant information;
    - Number of units (quantity);
    - Consignees and agents involved in transfer;
    - Reason for the denial;
    - Submission of pertinent marketing information;
- Information on the number and nature of investigations and enforcement actions, including types of technologies and conditions of violative behaviors.

We would furthermore encourage a classified annex on successful applications be made available to federal agencies, in addition to legislative oversight bodies.

The last component of effective implementation should be to conduct **recurring outreach to industry and civil society in order to ensure that federal agencies' efforts match the fast pace of technological development**, as well as to address changes in the methods used by infringing parties to bypass export controls and potential need for decontrolling technologies to promote legitimate research or information security objectives.