**Submission: The Surveillance Industry and Human Rights**

Access Now ([www.accessnow.org](http://www.accessnow.org)) is an international organization that defends and extends the digital rights of users at risk. We appreciate this opportunity to input into the Special Rapporteur’s consultation on the surveillance industry and human rights.

A global accountability crisis persists with regard to the development, marketing, sale, and use of private surveillance technology. We hope this submission contributes to efforts by all stakeholders to formulate and implement laws and norms to ensure these tools do not facilitate the infringement of human rights. We answer select questions from the Call for Submissions[[1]](#footnote-1), italicized below.

*A. Information concerning the domestic regulatory frameworks that may be applicable to the development, marketing, export, deployment, and/or facilitation of surveillance technologies by private companies, such as:*

*1. Laws, administrative regulations, judicial decisions, or other policies and measures that impose regulations on the export, import or use of surveillance technology;*

Currently, 42 states participate in the multilateral Wassenaar Arrangement, a voluntary body that sets norms on the trade of conventional arms as well as dual-use technologies.[[2]](#footnote-2) Its aim is to “contribute to regional and international security and stability, by promoting transparency and greater responsibility” in the transfer of controlled “listed” items. Particularly, the body intends to keep these powerful tools from those who would counter the coalition’s goals.

Participating states are meant to apply export controls to the agreed items in the List of Dual-Use Goods and Technologies and the Munitions List. Of the 42 states, only 22 appear to have provided the Wassenaar Arrangement website administrators with links to the relevant export controls as implemented by their governments.[[3]](#footnote-3) The agreement is voluntary, in that the decision whether to allow or deny the transfer of any item, including those on the Wassenaar Arrangement’s own lists, is the “sole responsibility” of the participating state. This has lead to inconsistencies for users, governments, and companies alike.

Below we highlight a few of the participating states’ control lists, oversight bodies, and mechanisms.

**European Union**

The history of EU export controls began by regulating weapons of mass destruction, and the proliferation of the components that make such weapons possible.[[4]](#footnote-4) Over time, technologies that trickled down from military use to civilian applications — like encryption — were included too. Today, a number of cyber-surveillance technologies characterized as “dual-use” have joined the list.

After surveillance technology was used to clamp down on Arab spring protests, international civil society organizations[[5]](#footnote-5) and EU parliamentarians called for a meaningful overhaul of export controls in an effort to restrict the ability of EU companies to provide repressive governments with the technology to infringe citizens’ rights.[[6]](#footnote-6)

In 2016, the European Commission proposed a review of the current export control system – the EU Dual Use Regulation – in order “to prevent human rights violations associated with certain cyber-surveillance technologies.”[[7]](#footnote-7) Regulators sought to modernise and simplify the existing system to limit the spread of technology used for surveillance. NGOs advocated for the strengthening of several of these proposed protections, including:

* strengthened human rights and due-diligence standards,
* broader scope to cover new and emerging surveillance technologies,
* greater reporting transparency and consistency,
* removal of export controls on encryption, and,
* protections for security research.

Many of these reforms were reflected, in some form, in the text adopted by the European Parliament in early 2018.[[8]](#footnote-8) For the review to be finalized, the European Parliament and the Council of Ministers, which represents the EU’s national member states, must still find agreement on a final text. For this to happen, member states must must attain a joint position, a process that has been stalled by economic interest and national security backdoor deals. We urge the EU to conclude this process as soon as practicable, and to place human rights, transparency, and accountability at the center of the system.

In October, leaked documents revealed how several member states were watering down the human rights protections which the European Commission and the Parliament proposed.[[9]](#footnote-9) As the internal documents from the German Government and EU Council show, a group of member states toppled the so-called “catch all” clause, a crucial safeguard requiring companies to inform the European Commission in cases where they identify human rights risks linked to their surveillance exports. Others, notably the UK, Sweden, and Finland, are pushing for weaker human rights protections, a dramatically less-inclusive controls list, and maintaining the existing, opaque practices for license disclosure and reporting.

**United Kingdom**

The UK publishes its own Strategic Export Control Lists.[[10]](#footnote-10) In terms of non-binding guidelines, the UK was the first government to release a National Action Plan on the implementation of the UN Guiding Principles on Business & Human Rights.[[11]](#footnote-11) The initial plan spoke to the export of surveillance technology, saying that all listed technologies undergo assessments that, “take full account of possible human rights impacts; a licence would not be granted if we judge there is a clear risk that the proposed export might be used for internal repression.”[[12]](#footnote-12) The plan committed to “develop guidance to address the risks posed by exports of information and communications technology that are not subject to export control but which might have impacts on human rights including freedom of expression online.” The guidance, developed by TechUK and published in 2014, studied exports to Bahrain as a part of its due diligence rubric.[[13]](#footnote-13) TechUK has continued contributing to the development of guidance[[14]](#footnote-14) and the UK has since updated its National Action Plan, trumpeting the TechUK guidance and 2013 Wassenaar rules on dual-use technologies.[[15]](#footnote-15)

It does not appear the UK’s laws or guidelines have had a measurable impact. According to freedom of information requests, the UK government granted more than 100 export licenses to over a dozen UK companies between early 2015 and mid 2016.[[16]](#footnote-16) Countries with records of gross human rights abuses appear in the records, as reported by Privacy International.[[17]](#footnote-17) To our knowledge, the United Kingdom has controlled the sale of at least one intrusion software product based on its use of cryptography.[[18]](#footnote-18)

**United States**

The United States Bureau of Industry and Security (BIS) maintains, as part of its complex Export Administration Regulations (EAR),[[19]](#footnote-19) the Commerce Control List (CCL)[[20]](#footnote-20) of items with specified export control classification numbers.

The U.S. maintains extensive regulations concerning surveillance and law enforcement and intelligence access to information, yet these laws allow for any number of activities with little to no limitations and/or oversight. With regard to hacking by the U.S. government, the U.S. Supreme Court recently approved controversial updates to the Federal Rules of Criminal Procedure, which remove limits on law enforcement hacking, arguably blessing U.S. hacking operations, including those that target computers en masse located around the world. Under the updated rule, a single warrant could be used to target not only criminals but also potentially millions of victims of botnet exploitation.[[21]](#footnote-21)

**Laws on the use of surveillance technology**

As for national laws governing the use of surveillance technologies, countries vary greatly.

Governments often lack meaningful surveillance laws that give proper notice about the activities they can undertake and why. Germany, which has been embroiled in several surveillance scandals over the past years, adopted a program which allowed law enforcement agencies to covertly install malware (trojans) to spy on its people.[[22]](#footnote-22) Only after details of the program came to light, Germany authorized it by law. Critics argued that not only does it constitute an invasion of privacy and endangers the integrity of the digital ecosystem; they also argued it costly and unnecessary for the level of investigations that it was rolled out for.[[23]](#footnote-23)

In contrast there are countries who have written comprehensive surveillance laws which allow for any number of activities with little to no limitations or oversight. One such example is the controversial Investigatory Powers Act which was rushed through legislature in the UK. The Law is so egregious that it has faced steady litigation by human rights groups, leading to a 2018 decision that the powers enshrined are in violation of EU law.[[24]](#footnote-24)

Surveillance at the local level in the U.S. demonstrates the proliferation of private surveillance technology, but also civilian and legislative efforts to increase oversight. Police departments across the U.S. employ private surveillance technology in their everyday operations and share data with private firms. Stingrays, also known as cell site simulators or IMSI catchers, are used by local police throughout the country,[[25]](#footnote-25) often under non-disclosure agreements with private vendors.[[26]](#footnote-26) The Chicago Police Department, for example, procures surveillance cameras, license plate readers, gunshot location services, biometric and facial recognition systems, and cell site simulators,[[27]](#footnote-27) while also enlisting owners of private closed-circuit cameras to share video footage with the City.[[28]](#footnote-28) New York City maintains a massive police department that enjoys a range of private surveillance technology, including drones,[[29]](#footnote-29) and has been shown to share surveillance data with private companies.[[30]](#footnote-30)

In response, cities and municipalities are beginning to pass legislation, dubbed “Community Control Over Police Surveillance” (CCOPS) laws, mandating civilian oversight of acquisition and even use of surveillance technology.[[31]](#footnote-31) For example, the New York City Council is considering a law that would require the police to notify the public and evaluate all surveillance technology it intends to acquire or use,[[32]](#footnote-32) while Oakland, California, went further to mandate police report on the actual use of such technology.[[33]](#footnote-33)

*2. Remedies available in the event of illicit export or use of private surveillance technology;*

All forms of government-sponsored hacking interfere with human rights. Many countries have national human rights institutions and commissions who monitor implementation of international human rights instruments. These bodies should be empowered to investigate and remedy illicit uses of private surveillance technology. In 2011, Frank La Rue, then the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, stated, in part, “When a cyber-attack can be attributed to the State, it clearly constitutes… a violation of its obligation to respect the right to freedom of opinion and expression.”[[34]](#footnote-34) International human rights instruments, like the International Covenant on Civil and Political Rights, the European Declaration of Human Rights, and the Universal Declaration of Human Rights, guarantee these rights, as well as rights to privacy, association, and due process, amongst others, which are all impacted by illicit use of private surveillance technology by states.

Despite the fact that most countries have laws and regulations governing communications surveillance, we are aware of very few affected groups or individuals who have achieved meaningful legal redress in practice for the illicit use of private surveillance technology by states. Lawsuits have been filed in various national courts,[[35]](#footnote-35) and some continue while others have been dismissed.[[36]](#footnote-36) Uncertain jurisdiction, corporate liability shields, sovereign immunity, lack of technical evidence, restrictive contracts, and official impunity all frustrate legal remedy. With some exceptions, the rule remains that courts do not provide relief for victims of the illicit use of private surveillance technology.

Attempts to use non-binding and norm-setting mechanisms have produced some results. The OECD maintains Guidelines for Multinational Enterprises (“Guidelines”) that encourage respect for human rights by the private sector. The Guidelines exhort companies to “[s]upport, as appropriate to their circumstances, cooperative efforts in the appropriate fora to promote Internet Freedom through respect of freedom of expression, assembly and association online.”[[37]](#footnote-37) The Guidelines also assert the need to protect privacy online, advising corporations to, “[r]espect consumer privacy and take reasonable measures to ensure the security of personal data that they collect, store, process, or disseminate.”[[38]](#footnote-38) Civil society have prompted inquiries by National Contact Points into specific cases where private surveillance tech purveyors infringed the Guidelines.[[39]](#footnote-39)

While we generally lack transparency into the export control application process and its outcomes, the few examples of authorities rejecting such applications appear to be the exception, rather than the norm. Hacking Team’s “global license” was revoked in Italy, some time after leaks of the firm’s data and the death of an Italian student in Egypt, a client country.[[40]](#footnote-40)

*B. Information concerning the use of such surveillance technologies:*

*1. Details of emblematic cases of State use of private surveillance technology against individuals or civil society organizations.*

In May 2018, Access Now released a report documenting the most recent known abuse of FinFisher technology against government critics in Turkey.[[41]](#footnote-41) The report provides up-to-date details on how FinFisher’s technology (made infamous after the company was breached by Phineas Fisher in August 2014) is currently being wielded against critics and evading scrutiny by security researchers, drawing on two years of observation.[[42]](#footnote-42)

Our documentation of FinFisher malware attacks reveals that the software is being used as part of “social engineering” campaigns designed to compromise mobile devices. After use of the company’s malware to crush dissent was first revealed, many researchers analysed multiple samples to document its capabilities. Two years ago, researchers could more easily map the company’s customers.[[43]](#footnote-43) The malware samples in our report show the company is placing more emphasis on obfuscation and non-attribution of its operational infrastructure. Our analysis of uses of FinFisher’s “FinSpy” for mobile devices exposed the attacks in Turkey, but also helped to identify other copies of the malware that indicate broader current use.

In the same report, we provided evidence of FinSpy use in concurrent efforts to undermine civil society outside Turkey, including the compromise of individuals in Indonesia, Ukraine, and Venezuela.

*2. Company policies to ensure that the development and sale of surveillance technologies meets human rights standards, particularly those articulated in the UN Guiding Principles on Business and Human Rights.*

Rights-respecting corporate policies and procedures are necessary, but not sufficient, to ensure surveillance technology development and sale meets human rights standards.

Larger companies, especially those coming from the more traditional telecommunications market, have developed commitments to not infringe upon human rights and to limit -- or fully restrict -- their role in enabling surveillance. While many of them do not develop surveillance technologies outright, the networks and systems they operate across the world have been used as a resource for surveillance activities by governments.

Nokia developed such a commitment in October 2016, stating in the Nokia Group human rights policy that “Nokia will not knowingly provide technology or services for the purpose of limiting political discourse, blocking legitimate forms of free speech, or otherwise contributing to activities that are not consistent with internationally recognized human rights standards.”[[44]](#footnote-44)

Similarly, on the human rights section of their website, Ericsson explicitly refers to the UNGP on business and human rights and gives a short profile of their internal compliance and due diligence processes. They state, “We identify and manage human rights issues in a number of ways, including Human Rights Impact Assessments (HRIA) in high-risk countries, stakeholder consultations in conjunction with HRIAs, and internal processes such as sales compliance and responsible sourcing.”[[45]](#footnote-45)

A host of companies endorsed the 2018 Paris Call for Trust and Security in Cyberspace, committing to, inter alia:

* Develop ways to prevent the proliferation of malicious ICT tools and practices intended to cause harm
* Strengthen the security of digital processes, products and services, throughout their lifecycle and supply chain
* Support efforts to strengthen an advanced cyber hygiene for all actors
* Take steps to prevent non-State actors, including the private sector, from hacking-back, for their own purposes or those of other non-State actors.

These sorts of commitments must be complemented by with regular expert, independent, third party assessment, empowered oversight and review boards, and redress mechanisms. Still, this would only serve as the basis for accountability of technology companies towards human rights. Such tools and structures are not enough to fully address the deep and persistent human rights violations facilitated by private surveillance technology.[[46]](#footnote-46) Time and experience have proven that voluntary compliance cannot substitute for proper regulation and enforcement, as victims of surveillance technologies have often been left with no legal framework to defer to when they are faced with a violation of their rights.[[47]](#footnote-47)

**Disposals, makeovers, and accountability**

In a move referred to as “disposals” or “makeovers,” some private firms spin-off controversial arms after public criticism of the mother or previous company’s human rights practices. These corporate maneuvers often compound the difficulty victims face in finding accountability or remedy for the illicit use of private surveillance technology, as the new, smaller firms swiftly alter their names, headquarter location, jurisdiction, investors, and ownership.

Nokia Siemens disposed of its surveillance arm in March 2009, following allegations of Nokia Siemens’ monitoring systems contributing to the Iran government’s crackdown on the Green Movement. Nokia Siemens sold the business division responsible for surveillance technology, Intelligence Solutions and its new owners, Perusa Partners Fund 1 LP, renamed the business unit as Trovicor.[[48]](#footnote-48) Likewise, Chinese telecoms giant ZTE discarded its ZTESec wing in 2012 after links to Iran were exposed; the new firm was renamed SinoVatio, but retained ties to ZTE, including the same mailing address as a wholly-owned ZTE development firm.[[49]](#footnote-49) For its part, the British firm Gamma Group was associated with FinFisher, which now appears to originate from Germany.[[50]](#footnote-50)

More recently, U.S. venture capital firm Francisco Partners succeeded in selling Israeli surveillance tech firm NSO Group for a hefty profit,[[51]](#footnote-51) even after extensive reporting on human rights violations committed by multiple governments using NSO Group products.[[52]](#footnote-52) This move follows a previously attempted sale that was aborted under civil society pressure and institutional investor advocacy.[[53]](#footnote-53)

Disposals and makeovers can obstruct access to remedy for affected persons and infringe the human rights of those who continue to be victimized by the disposed entity’s activities. The maneuvers can increase the difficulty for victims to identify the parties responsible, to attach liability in the appropriate jurisdiction, and to find corporate accountability. Disposals and makeovers enable further transgressions, particularly as spin-off companies tend to be privately held, renamed, and removed from public oversight.

Yet, in their study of the Second Pillar of the UN Ruggie “Protect, Respect, Remedy” Framework and business relationships, the Institute for Business and Human Rights notes “companies may find that disposal does not always end their association with an asset they have sold.”[[54]](#footnote-54) Current efforts to construct a binding international treaty on business and human rights in part stem from the inability to hold accountable companies who have disposed of or acquired rights-infringing assets.[[55]](#footnote-55)

*3. The extent to which private surveillance companies offer services to States and other actors to deploy their technologies in specific circumstances, and the extent to which companies are aware of the end-use of the technologies they market.*

Surveillance companies often market themselves as a tool for law enforcement and state agencies to carry out investigations. This is clearly stated on their promotional materials and websites without going into any further detail on the responsible deployment of the tools they provide. Their logic is that it is not their place to question the intelligence or law enforcement objectives of the governments, and they generally leave the legality of their tools for the governments to address within themselves. Popular tools like Cellebrite which are a known, widespread tool used by agencies around the world, propose no precautions or suggestions about how to deploy the technology they provide in line with human rights standards.[[56]](#footnote-56)

The viability of this strategy has been proven by a stream of “hacking companies” who have gone on to successfully rebrand and resell their products with this exact framing. The most recent which comes to mind is the Hacking Team’s rebrand to Grey Heron technologies -- which aims to provide “lawful access” to the most popular encrypted services.[[57]](#footnote-57)

To verify such marketing claims, and ensure these powerful, invasive, and secretive tools are intended and developed for only specific and lawful purposes, an international agreement and certification process such as the Montreux Document and International Code of Conduct Association (ICoCA)[[58]](#footnote-58) serves in the private security sector could be a starting point for discussions of regulation of the analogous private surveillance space.

**Conclusion**

A global accountability crisis persists with regard to the development, marketing, sale, and use of private surveillance technology. Comprehensive regulation and corporate safeguards are both urgently necessary to protect privacy, freedom of expression, and other fundamental rights being infringed by states’ illicit use of private surveillance technology. Yet core questions of jurisdiction, corporate liability shields, sovereign immunity, contractual restrictions, and official impunity could continue to frustrate efforts to prevent, mitigate, and remedy illicit sale and use.

We recommend that the Special Rapporteur deeply consider the difficulty of holding either the private purveyors or the responsible governments to account thus far, and to seek a holistic and rights-responsive framework that can begin to meaningfully address the problem through inclusive and innovative accountability measures.

\*\*\*

*For more information, contact:*

Peter Micek

General Counsel

Access Now | www.accessnow.org

peter@accessnow.org

+1-888-414-0100 x709

1. https://freedex.org/2018/12/13/call-for-submissions-the-surveillance-industry-and-human-rights/ [↑](#footnote-ref-1)
2. https://www.wassenaar.org/about-us [↑](#footnote-ref-2)
3. See https://www.wassenaar.org/participating-states. [↑](#footnote-ref-3)
4. http://ec.europa.eu/trade/import-and-export-rules/export-from-eu/dual-use-controls/ [↑](#footnote-ref-4)
5. See https://www.fidh.org/en/issues/globalisation-human-rights/cause-coalition-calls-on-eu-to-update-dual-use-regulation-to-protect. [↑](#footnote-ref-5)
6. See https://www.euractiv.com/section/digital/news/parliament-calls-for-stricter-controls-over-surveillance-tech-exports/. [↑](#footnote-ref-6)
7. See <http://europa.eu/rapid/press-release_IP-16-3190_en.htm>. [↑](#footnote-ref-7)
8. See <https://www.euractiv.com/section/cybersecurity/news/meps-approve-export-controls-tailored-to-stop-government-surveillance/>. [↑](#footnote-ref-8)
9. See https://netzpolitik.org/2018/surveillance-exports-how-eu-member-states-are-compromising-new-human-rights-standards/. [↑](#footnote-ref-9)
10. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/766972/UK\_Strategic\_Export\_Control\_Lists\_20181219.pdf [↑](#footnote-ref-10)
11. https://www.business-humanrights.org/en/uk-national-action-plan-implementing-un-guiding-principles-on-business-and-human-rights-0#128162. [↑](#footnote-ref-11)
12. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/236901/BHR\_Action\_Plan\_-\_final\_online\_version\_1\_.pdf. [↑](#footnote-ref-12)
13. http://www.techuk.org/images/CGP\_Docs/Assessing\_Cyber\_Security\_Export\_Risks\_website\_FINAL\_3.pdf. [↑](#footnote-ref-13)
14. https://www.techuk.org/insights/news/item/10296-cyber-security-export-controls-recast-of-eu-export-control. [↑](#footnote-ref-14)
15. See https://globalnaps.org/country/united-kingdom. [↑](#footnote-ref-15)
16. https://motherboard.vice.com/en\_us/article/4xaq4m/the-uk-companies-exporting-interception-tech-around-the-world. [↑](#footnote-ref-16)
17. https://motherboard.vice.com/en\_us/article/8q8vek/data-shows-how-the-uk-grants-licences-to-export-interception-tech-imsi-catchers. [↑](#footnote-ref-17)
18. https://privacyinternational.org/legal-action/r-application-privacy-international-v-commissioner-hm-revenue-customs-gamma-finfisher [↑](#footnote-ref-18)
19. See <https://www.bis.doc.gov/index.php/regulations/export-administration-regulations-ear>. [↑](#footnote-ref-19)
20. See https://www.bis.doc.gov/index.php/regulations/commerce-control-list-ccl. [↑](#footnote-ref-20)
21. See https://motherboard.vice.com/en\_us/article/yp3kz5/us-judges-can-now-sign-global-hacking-warrants. [↑](#footnote-ref-21)
22. See https://www.dw.com/en/german-federal-police-use-trojan-virus-to-evade-phone-encryption/a-42328466. [↑](#footnote-ref-22)
23. See <https://www.dw.com/en/things-to-know-about-germanys-recent-surveillance-laws/a-39421060>. [↑](#footnote-ref-23)
24. See https://www.theguardian.com/technology/2018/apr/27/snoopers-charter-investigatory-powers-act-rewrite-high-court-rules. [↑](#footnote-ref-24)
25. See https://www.aclu.org/issues/privacy-technology/surveillance-technologies/stingray-tracking-devices-whos-got-them. [↑](#footnote-ref-25)
26. See <https://www.techdirt.com/articles/20180120/06352239048/harris-stingray-nondisclosure-agreement-forbids-cops-telling-legislators-about-surveillance-tech.shtml>. [↑](#footnote-ref-26)
27. See e.g. https://redshiftzero.github.io/policesurveillance. [↑](#footnote-ref-27)
28. See https://www.chicago.gov/city/en/depts/oem/provdrs/tech/svcs/link\_your\_cameras.html and https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html. [↑](#footnote-ref-28)
29. See <https://www.nytimes.com/2018/12/04/nyregion/nypd-drones.html>. [↑](#footnote-ref-29)
30. See https://theintercept.com/2018/09/06/nypd-surveillance-camera-skin-tone-search. [↑](#footnote-ref-30)
31. See https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance. [↑](#footnote-ref-31)
32. See <https://www.brennancenter.org/analysis/public-oversight-surveillance-technology-post-act-resource-page> and https://www.eff.org/deeplinks/2018/10/lifting-cloak-secrecy-nypd-surveillance-technology. [↑](#footnote-ref-32)
33. See https://arstechnica.com/tech-policy/2018/05/oakland-passes-strongest-surveillance-oversight-law-in-us. [↑](#footnote-ref-33)
34. See UN Doc. A/HRC/17/27, May 16, 2011, ¶ 52, available at <http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf>. [↑](#footnote-ref-34)
35. See, e.g., <https://apnews.com/a5d4f292925348ceaf64f649b4f79a0f> & <https://www.theguardian.com/world/2018/oct/11/bahraini-arab-spring-dissidents-sue-uk-spyware-maker>. [↑](#footnote-ref-35)
36. See, e.g., <https://www.eff.org/cases/kidane-v-ethiopia>. [↑](#footnote-ref-36)
37. See http://mneguidelines.oecd.org/guidelines. [↑](#footnote-ref-37)
38. Org. for Econ. Dev. & Coop, Guidelines for Multinational Enterprises (2011), http://mneguidelines.oecd.org/2011ConsumerInterests.pdf. [↑](#footnote-ref-38)
39. See https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\_data/file/402462/BIS-15-93-Final\_statement\_after\_examination\_of\_complaint\_Privacy\_International\_and\_Gamma\_International\_UK\_Ltd.pdf. [↑](#footnote-ref-39)
40. See <https://motherboard.vice.com/en_us/article/78k8dq/hacking-team-has-lost-its-license-to-export-spyware>. [↑](#footnote-ref-40)
41. Access Now, *FinFisher Changes Tactics to Hook Critics* https://www.accessnow.org/cms/assets/uploads/2018/05/FinFisher-changes-tactics-to-hook-critics-AN.pdf [↑](#footnote-ref-41)
42. https://securityzap.com/a-story-of-a-finfisher-hacker/ [↑](#footnote-ref-42)
43. https://citizenlab.ca/2015/10/mapping-finfishers-continuing-proliferation/ [↑](#footnote-ref-43)
44. https://www.nokia.com/sites/default/files/Nokia\_Group\_Human\_Rights\_Policy.pdf [↑](#footnote-ref-44)
45. https://www.ericsson.com/en/about-us/sustainability-and-corporate-responsibility/responsible-business/human-rights [↑](#footnote-ref-45)
46. See https://www.accessnow.org/nokia-revamps-human-rights-policy-pledging-avoid-active-surveillance/. [↑](#footnote-ref-46)
47. Nokia itself faced such an issue on the back of a surveillance case in Iran <<https://www.zdnet.com/article/nokia-siemens-networks-respond-to-iran-human-rights-abuses-claims/>>, but there are many cases of surveillance companies which claim compliance, but end up in violation only to be let off the hook because of the absence of a legislative framework. The case of Gamma International is often cited as an example of this systemic breakdown <https://www.theregister.co.uk/2015/02/26/oecd\_rules\_anglogerman\_finfisher\_spyware\_violated\_human\_rights/>. [↑](#footnote-ref-47)
48. http://web.archive.org/web/20130328104247/http://blogs.nokiasiemensnetworks.com/corporate-responsibility/2009/06/22/provision-of-lawful-intercept-capability-in-iran/ [↑](#footnote-ref-48)
49. See <https://www.reuters.com/article/us-zte-security-subsidiary/under-fire-zte-sells-surveillance-systems-subsidiary-idUSBRE89F0EI20121016> and https://flashcritic.com/chinese-telecom-links-to-intelligence-disclosed. [↑](#footnote-ref-49)
50. See e.g. <https://thehackernews.com/2017/09/gamma-finfisher-hacking-tool.html> and https://www.accessnow.org/new-report-finfisher-changes-tactics-to-hook-critics. [↑](#footnote-ref-50)
51. See [https://calcalistech.com/ctech/articles/0,7340,L-3756381,00.html](https://calcalistech.com/ctech/articles/0%2C7340%2CL-3756381%2C00.html). [↑](#footnote-ref-51)
52. See, e.g. https://www.nytimes.com/2018/08/31/world/middleeast/hacking-united-arab-emirates-nso-group.html. [↑](#footnote-ref-52)
53. See <https://finance.yahoo.com/news/digital-rights-groups-pressure-blackstone-reported-nso-group-173520579--sector.html> & <https://www.accessnow.org/blackstone-wont-invest-nso-groups-toxic-spyware>. [↑](#footnote-ref-53)
54. See IHRB, State of Play: The Corporate Responsibility to Respect Human Rights in Business Relations (at Ch. 6) http://www.ihrb.org/pdf/state-of-play/ State-of-Play-Full-Report.pdf. [↑](#footnote-ref-54)
55. See https://www.accessnow.org/four-years-to-a-first-draft-slow-progress-toward-treaty-to-bind-companies. [↑](#footnote-ref-55)
56. See https://www.cellebrite.com/en/about/company. [↑](#footnote-ref-56)
57. See <https://motherboard.vice.com/en_us/article/bj54kw/grey-heron-new-spyware-brochure-hacking-team>. [↑](#footnote-ref-57)
58. See https://www.icoca.ch/en [↑](#footnote-ref-58)