Export Control of Surveillance Software from Germany and Europe - Regulations, Limits and Weaknesses

Explainer

In a reality where mobile devices have become a core element of contemporary life, communication and the expression of personal interests and relationships, the covert amassing of this information has become an interest of state actors that are willing to spy on their citizens (and worse). As this task is hard to accomplish, companies have arisen that provide and sell this service, often with a questionable understanding of the impact on human rights. At the same time, regulation of the export of such tools and services is problematic and the current legal basis in the EU, which is the focus of this text, leaves many loopholes for its circumvention. The upcoming revisited EU export control regime is trying to close these loopholes, but many issues remain, which the present paper aims to address.

Introduction or “The Relation Between Smartphones and Human Rights”

My Smartphone is my life. Not literally, of course, but it contains nearly all my private and work contact information: I use it for much of the written communication that comes with my job, read papers and query the internet on it, and use it for phone calls. I am quite sure that many others behave similarly. And where I still sometimes refrain from certain activities, my children won’t even know a world with this distinction and without an always-on connection to their friends, relatives, and – in a few years – their work colleagues. This concentration of so many central aspects of our personal life and thus of our friends and colleagues on a single technical device creates problematic conflicts of interests. In recent years, many incidents have shown that intelligence services and security agencies in democratic and not-so-democratic states are willing to break the “digital seals” and security measures that are intended to protect users’ personal information and the data stored on these devices. Even if this protection might here in the EU seem like a “luxury problem” – as reflected in the debates and complaints regarding the GDPR and the associated extra work required, for example, of companies – in some regions of the world it directly and prac-
The Shadowy Business of Hacking Smartphones

Unfortunately, the demands to acquire such information secretly and without the target's knowledge have developed into a money-making business. Since modern smartphones are quite secure and popular apps often provide end-to-end encrypted information transfer, making wire-tapping difficult if not impossible, the knowledge of how to access the devices directly in order to intercept information on the device itself is rare and valuable. It is therefore not surprising that companies have developed that specialize in providing this knowledge or offer the service of hacking directly into specific devices. Officially, they provide these services only to state customers, in compliance with legal commitments and regulations for law enforcement or anti-terrorism efforts. A few of these companies are based in the EU, such as FinFisher in Germany, the former Hacking Team from Italy (which is now part of Italy-based Memento Labs), or the former company Vupen in France (now part of EU/US-based Zerodium). Some companies like Vupen/Zerodium acquire and sell information disclosing weaknesses or security problems in prominent hardware or software that can be used by buyers to circumvent security measures or otherwise exploit them. Others, like FinFisher or Hacking Team provide, sell, or rent software that is capable of breaking into devices, acquiring stored information and intercepting communication. Although such services and products are regulated under an EU export control regime due to their human rights implications and are implemented according to national law, FinFisher and Hacking Team, in particular, have been in the headlines several times for selling their products to states that used them to spy on political opposition candidates and human rights activists or target journalists, sometimes with fatal consequences for these individuals. These and other incidents highlight the dilemma of the current regulatory approaches in the EU towards such critical software.

The Regulation of Critical Software and Hacking Services in The EU

The EU included the regulation of such network surveillance and intrusion software in its list of regulated dual-use items in 2014, taking into account that these products can have a legitimate civil application (the Wassenaar Arrangement made a similar assumption in 2012 and 2013). Furthermore, the EU export control regime requires states to validate export requests and deny them if “there is a clear risk that the [...] equipment to be exported might be used for internal repression” taking into account “all relevant considerations” including its possible usage for activities that might violate human rights. This sounds like a strong and clear “basic rule” for export licensing, but it is actually far more complex. Due to the national implementations, considerations often have different outcomes in different EU member states. Some states might also regard other priorities such as national economic growth, support for a dedicated national technological field of expertise, or the influence on the political relationship with the receiving country. And even if all these aspects are considered in good faith and with a focus on human rights, it is difficult to control the actual usage of software or – the other way around – to prevent it from being used outside the conditions and constraints of an export permission. As a virtual product, software is easily distributable and duplicatable, unlike physical goods that can be touched, tracked, and counted. In addition, these kinds of products are officially designed and marketed for security and law-enforcement purposes; they are even undeniably required for certain use cases and scenarios. Some countries, such as Germany, even declared this economic branch as a national key technology in connection with the decision to foster and support national companies achieve economic success. Finally, the sheer speed of the technological advancements of communication tech-
nologies is accompanied by an equally rapid development of surveillance technology, whereby every approach to explicitly listing export-regulated items is doomed to constantly become outdated and incomplete.

**Important Changes and Existing Challenges of the Upcoming Revisited EU Regulation**

The upcoming revised version of the EU export control regulation aims to ease some of these problems. An important measure is the inclusion of a “catch-all” approach, which extends the use of a list-based control regime with an additional assessment of new technologies regarding the export control principles and guidelines, especially human rights considerations. The assessment includes stronger cooperation and information sharing between member states regarding new technological developments and their export control relevance. This comprehensive assessment could become a strong tool, as it allows for the support of NGOs, academia, and other public actors as early-warning detectors regarding the impact of upcoming technologies on human rights, mitigating the problem of running after new developments with fixed lists. The revised export control regime furthermore includes an obligation to produce annual reports of national exports. This mechanism can help establish an EU-wide common ground and understanding of critical exports, on condition that reporting is carried out extensively, regularly and with care, that is not undermined by national interests. However, the concerns of control being compromised by national self-interest or diverging approaches based on the domestic interpretation of regulations, in particular, remain, as the revised version still leaves the opportunity for states to add their unique national licensing requirements. As custom regulations weaken the effectiveness of an EU-wide export regime, overcoming such national peculiarities should be the goal of any further upcoming changes. As the new regulation puts a major part of the decision about what requires licensing in the hands of the exporter, it is even more relevant to limit the room for interpretations and make exporting manufacturers provide truthful and verifiable statements regarding the human-rights related, critical capabilities of their products. To achieve this, the EU could prepare and share a common set of parameters and questions regarding the specific technical capabilities of an assessed product that goes beyond the mere self-declarations and lip service required during the export licensing process. Of course, this requires regulatory authorities to maintain a strong(er) technical understanding of critical software. Finally, the problem of limiting the actual usage of exported surveillance software remains. Given the already existing technical difficulties in tracking virtual goods, any effective measure would require the control and tracking of the exported software in each recipient country. On one hand, this also implies the need for bilateral cooperation beyond the actual export, possibly requiring ensuring that there is a legal basis for such measures within the receiving country, effective law enforcement to ensure the obligations as well as an overall willingness to undertake such measures. Alternately? Or “At the same time”?; such legal regulations, as well as the establishment of an effective end-user control in combination with the obligation for transparency and reporting measures, could be made a requirement for the export of critical software goods and, if established, could prove to be the strongest tool.

**Outlook and Why Cooperation Matters for Export Control**

Despite all this criticism, the revised EU export control regime could become an important step towards regulations that underline and practically strengthen the relevance of human rights considerations within the export licensing process. But as with many other EU decisions, its effectiveness will depend on the extent to which member states are willing to interpret and enforce these common rules uniformly and to avoid short-sighted policies driven by national self-interest.
Further Reading


The opinions expressed in this text are solely that of the author/s and do not necessarily reflect the views of the Heinrich Böll Foundation and/or of the Israel Public Policy Institute (IPPI), their staff, trustees and/or the organizations that support their work.

30 December 2021
by Thomas Reinhold

© Heinrich-Böll-Stiftung e.V.
Schumannstraße 8
10117 Berlin
T +49 (30) 285 34-0
F +49 (30) 285 34-109
www.boell.de
info@boell.de