DE GRUYTER
OPEN

Technology Transfer in the EU: Exporting Strategically Important ICT Solutions to Other EU Member States

Anni Säär

Estonian Human Rights Centre
Narva mnt 9j,
Tallinn 10117, Estonia
E-mail: anni.saar@hotmail.com

Addi Rull

Tallinn Law School,
Tallinn University of Technology
Akadeemia tee 3,
Tallinn 12618, Estonia
E-mail: addi.rull@ttu.ee

Abstract: *The fast development of ICTs pose new challenges to the European Union and its Member States. Every EU country has its own policies regarding technology transfer, ownership of state e-services, and the possibilities how the state-owned or licensed e-service could be exported. Taking into account the free movement of goods, the EU has created a platform to cooperate and export IT solutions. However, the lack of preparedness of infrastructures, legislation and stakeholders for cross-border exchanges poses a threat to IT transfer and should be taken into consideration in the EU as well. In the coming decades the number of outsourced ICT solutions, strategically important ICT solutions, public services and critically important information exchange platforms developed on behalf of the states, will grow exponentially. Still, digital development is uneven across the EU, they grow at different speeds and the performance is quite splintered. There are legal provisions which are outdated and therefore impede technological cooperation and export of IT solutions. A Member State may restrict the ICT licensing based on national security and policy reasons and the ownership of intellectual property might pose a threat to technology transfer or further development of the IT solution. There are examples of strategically important export of ICT solutions, the experience at which can be*

expanded to cover other EU Member States. Strong collaboration would enable mutual learning from past experiences along with the opportunities for better use of technology. Parallels can be drawn with military technology transfers, as the policies and legal framework was first developed and mostly used with them.

This introduces a question of what are the conditions for exporting strategically important ICT solutions from one Member State to another, given that there is no common legal framework developed yet, and who should decide whether to transfer or not?

Keywords: *computer programs, e-services, export of e-services, export of ICT solutions, intellectual property, strategically important ICT solutions, technology transfer*

1. Introduction

Free movement of goods and services in the European Union has created a competitive internal market for the benefit of European citizens and businesses. The internal market generates growth through innovation, mobility and competitiveness. Articles 28, 29 and 30 of the EC Treaty stipulate the content and scope of free movement of goods by prohibiting unjustified restrictions inside the internal market of the European Union. The fast development of information communication technologies (ICTs) pose new challenges to the European Union and its Member States. In the coming decades the number of outsourced IT solutions, public services and critically important information exchange platforms such as X-Road in Estonia, developed on behalf of the states, will grow exponentially. Countries use ICT to speed up the communication between different authorities and improve communication between the citizens and the state. States benefit from using ICT by reducing expenses and simplifying the work of the state apparatus. Nevertheless, digital development is uneven across the EU, they grow at different speeds and although in some areas the output is alike in other areas, as in the area of Digital Public Services, the performance is quite splintered (Council of European Union, 2015, p. 27). This introduces a question of what are the conditions for exporting strategically important ICT solutions from one Member State to another, given that there is no common legal framework developed yet.

The possibility to share ICT solutions between Member States avoids unnecessary duplication of research and developments, increases efficiency,

speeds up migration to digital public services and gives stronger bases for competition with Asia and America. Such developments are the prerequisites of maximising the Big Data possibilities which could increase GDP in the future. Technology transfer agreements refer to licensing, but it might happen that the developed technology is not so easy to license to another country. A Member State may restrict the technology licensing based on national security and policy reasons. Therefore, the future policy should take into account two main legal aspects. Firstly, how executive state authority can make legitimate decisions regarding strategically important state-owned ICT assets. The scrutiny of public law regulating state assets is necessary in order to determine the existence and the scope of delegating norms that facilitate the decision-making about the export of ICT assets. Secondly, the intellectual property policy for the public procurement of ICT solutions has to be determined so that it allows a state to export ICT assets and, generally, not to prevent developers from using the knowledgebase created during the work, because this is an important input for further ICT innovation.

Similar issues have been addressed in military technology transfer agreements. International military technology transfer must be consistent with national security and foreign policies. The difference between military technology and ICT is that in the latter case it is mostly a service or functionality which typically affects everybody as all of them are users. Only a certain part of ICT solutions pose a security risk and generally the risk is the data itself not technology as such. Military technology and products are the subjects of state's strategic interests, which are outside of public sales and consumption. ICT solutions, on the other hand, are mostly in public consumption and companies as well as private persons benefit from it. Therefore, the procedure of making export decisions regarding ICT solutions should be simpler than in the field of military technology. Nevertheless, military technology transfer is a useful parallel which must be analyzed as well.

The first section of the article discusses strategically important IT solutions and the subject of this article. The second section gives an overview of how intellectual property rights affect international technology transfer. International technology transfer is covered in the third section. Given the fact that military technology agreements have been developed and used effectively for years, the fourth section demonstrates how it has been done and what have been the main problems regarding the transferring. Based on the experience, the authors discuss what should be avoided and what have been the best practices in exporting strategically important IT solutions to other countries. In the fifth section, Estonian legislative environment regarding

exporting e-services is analyzed. Estonia has the experience of exporting some e-services, one of the most important of which is the X-Road which allows public and private sector e-services databases to connect and work in harmony (E-Estonia, 2013). The sixth section explains how the X-Road was exported and what steps were taken. The state outsources a system and IT companies will develop that system in other countries but the relationship and the intellectual property rights between the two parties have to be regulated. The final section of the article proposes conclusions and suggestions on how to encourage the exporting of e-services.

2. Strategically important ICT solutions

Living in an information society means that information is an indispensable asset and IT is widely used in all areas of life. Private sectors' interaction with the public sector can be considerably developed and made more operative by using digital technologies. Using electronic systems, for example in health systems and public procurements, streamlines processes, improves efficiency of systems and transparency. (Council of European Union, 2015) Technological advancements allow substantial leaps in the quality and speed of cross-border delivery and communication of goods and services (Hsu, 2010, p. 697). Though all of them have benefits, not all can be titled to be strategically important. Strategically important ICT solutions have to face national security and interests, they have to be necessary for the purpose of exercising state authority, and compromising those IT systems would constitute serious loss to the state.

An ICT solution, which is a computer program, consists of source code and object code. Source code is a program written by a programmer in a high level human readable language that tells a computer what to do (Stephen & Sumner, 1996, p. 180; Lin, Sag & Laurie, 2002, p. 238). Source code is written in certain programming languages such as Java, Cobol, Delphi, Basic, C, C++, C# or Pascal. Source code instructions must be translated or converted into object code before the computer can act upon them, only instructions expressed in object code can be used "directly" by the computer (*Apple Computer Inc. v. Franklin Computer Corporation* [1983]). Source code can be altered, understood or misappropriated by skilled programmers whereas object code is very problematic, if not impossible, to understand by visual inspection (Frankel, 2012, p. 275). Object code is a binary code written in a machine language, using 1's and 0's, which a processor can understand but for a human is difficult to

modify or read. To fully protect a computer program from use by another, both source and object code must be protected (Canfield, 1984, p. 419).

Simple automation of the existing services will not bring out the full benefits of the use of ICT in the information system, but reinventing service delivery and changing service processes will (E-Governance Academy, *n.d.*). E-services and digital environments are a crucial part of e-government and countries are interested in developing those. Public service is a fundamental institution of administrative law and it constitutes an activity that a state or a private party authorised by the state are doing to meet the social needs of public interest (Vedinas, 2012, p. 6). State-owned ICT solutions can be divided into two:

1) An IT solution which is a service but might not be strategically important. For instance, e-Prescription, which is part of the e-Healthcare system, for handling and issuing medical prescriptions. A doctor writes out a prescription electronically with the aid of an online form and at the pharmacy only an ID card is needed to release the prescribed medicine. All pharmacies and hospitals are connected to the system and, in 2013, 95 per cent of all prescriptions in Estonia were issued electronically (E-Estonia, *n.d.*, b). The e-Prescription system draws on data from the national health insurance fund, displaying also any state medical subsidies that the patient is entitled to, and the medicine is discounted accordingly (E-Estonia, *n.d.*, b). Therefore, the system without the data is not strategically important.
2) A strategically important ICT solution, such as the ID card system, which is the most highly-developed national ID card systems in the world. "The chip on the card carries embedded files which, using 2048-bit public key encryption, enable it to be used as definitive proof of ID in an electronic environment." (E-Estonia, *n.d.*, a) The chip includes asymmetrical processor supporting cryptosystem and at least 8kB EEPROM memory (Sepp, 1999). The ID card system provides basis for the development of secure e-services and therefore holds strategic importance to the country.

When considering the transferring of strategic technology, a country should think about the interests of the state and public. It has been suggested that if the country wishes to protect the transferrable technology, it should be exported to other countries only under special conditions and, if possible, seek full access to the markets of those countries in a way that the technology-supplying company (in this case, an IT company) may possibly achieve a market share (Levine, 1986, p. 373). Both the interests of the state and the possible advantage as well as benefit for the IT-company and the state itself would be covered by these suggestions.

In the current article the terms export and technology transfer are being used as synonyms.

> *Technology transfer is the transfer of systematic knowledge for the manufacture of a product, for the application of a process or for the rendering of a service, and is substantially completed by means of assignment, sale and licensing of all forms of technology property or technological achievements* (Ma, 2010, p. 16).

Therefore, besides an ICT solution, a computer program, knowhow, consultation services and customisation of the system are provided. Broadly it means an export of the product, the ICT solution, as well as related collateral services. On the other hand, when we talk about exports of regular computer programs then knowhow and technology transfer, that is, handing over the source code, are usually not included. For example, Microsoft products are not custom made and are released with user licence. Nevertheless, a computer program developed and outsourced by a government order is custom-made and therefore it is accompanied by technology transfer.

Generally, intellectual technology transfer covers computer programs but it may include also databases. Law distinguishes between computer programs and databases although both are subject to copyright protection. Accordingly, a database does not include an underlying computer programme that is needed to run it. Also, the content of a database is subject to separate protection. However, computer programs and databases become technically related in practice. The architecture of arrangement, organisation and systematisation of data, which is the essence of database protection, becomes naturally a component of a computer program. This is particularly the case when developing a digital solution of a state register. For instance, Estonia has approximately 600 hundred of registers (see, e.g., Rull, Täks & Norta, 2014, pp. 75–77). The Population Register is an example of one of the most used state databases. Usually, a content of a state database is not copyright protected, because it consists of non-protected elements such as factual data. In the European Union, databases are protected by copyright law as original works or by sui generis right accorded to investments made by database producers. If a database does not fall under these protection mechanisms, then it can be successfully protected by regular provisions of contract law (see, e.g., *Ryanair Ltd. v. PR Aviation BV* [2015]).

3. Intellectual property rights and licensing

Intellectual property rights provide protection against leakage of new technical information and give legal basis for revealing the proprietary characteristics of technologies (Maskus, 2004, p. 2). The content of contemporary intellectual property law originates from the 1883 Paris Convention for the Protection of Industrial Property and the 1886 Berne Convention for the Protection of Literary and Artistic Works. Intellectual property rights cover copyrights, trademarks, patents, industrial designs, plant variety rights, layout designs and geographical indications. Computer software as well as database creation can be particularly complex and costly, while copying the results is fairly simple and therefore protection of these is extremely important (Durell, 2000, p. 238). For example, the most expensive video game produced so far seems to be Destiny, which cost 500 million dollars to make (Curtis & Hoggins, 2014), followed by Grand Theft Auto 5, with marketing and developing budget of 265 million dollars (Villapaz, 2013). The cost and complexity of a computer program depends on the product itself; sometimes all it needed was a team and a good idea. Computer programs are protected under patent, copyright, trade secret and sui generis database laws.

Trade secret can be the best means of protection for a computer programme as it only requires taking reasonable legal and technical measures to keep the information, i.e. source code, secret. Non-disclosure and noncompetition agreements are examples of such legal measures. Technical measure is already fulfilled when a computer programme is made available only in object code. Decompiling object code into source code is prohibited aside from a few exceptions, such as, for example, the purpose of achieving interoperability between computer programmes. First, a vendor always has to exhaust all other possibilities to get instructions or necessary source code from the owner of the computer programme before he may resort to the process of decompiling the object code for the purpose of retrieving needed information. A successful decompilation never reveals the original source code one hundred per cent and the law prohibits the use of information for any other purposes except for the purpose of interoperability only. This makes it impossible for others to read the source code or to understand how a computer programme was written. Often the protection of source code as trade secret is favourable, because one can make a computer programme public only in object code while keeping the underlying information secret. This makes it possible to sell or license a computer programme without waving a trade secret. Trade secret law safeguards inventors more inexpensively and easily than patent protection (Rowe, 2009, p. 2).

Patents provide exclusive rights for twenty years and play a big role in international technology transfer (Dunning, 2013, p. 10). They offer a legal basis for revealing the proprietary characteristic of technologies to subsidiaries and licensees, supporting the formation of contracts (Maskus, 2004, p. 2). In a patent application, in order to receive a patent, the technical information about the computer program must be disclosed. But some technologies are not patentable and it might be that in one jurisdiction the technology is patentable and in another it is not. Although Article 52, Paragraph 2(c) of European Patent Convention stipulates that patents should not be granted for computer programs the patent protection in EU cannot be excluded solely on the grounds that a computer program was used. An invention would be patentable based on conventional patentability criteria and it should not be denied protection due to the mere fact that a computer program was used (Vicom, 1986, p. 16). It was specified on 1 July 1998 by EPO that a computer program product is not excluded from patentability under Article 52, Paragraphs 2 and 3 of the European Patent Convention if, when run on a computer, it produces a further technical effect which goes beyond the normal physical interactions between software and hardware (IBM, 1998, p. 13). Traditionally, in the US software has not been seen as patentable and the Patent Office has rejected software-based patent applications on different grounds (Scott, 2006, pp. 3–24.1). Due to the broad interpretation of patent law by the American justice administration in relation to a non-existent exclusion of computer programs from patentability as well as numerous and very diverse precedents has led to unlimited patenting of software on the territory of the United States (Szattler, 2007, p. 98).

Copyright protection of computer programmes is obtained automatically without the need for registration or other formalities. The automatic protection is obtained because copyright law treats computer programmes as literary works which are composed of written code, commands, notes, system architecture, and design (Durell, 2000, pp. 232–233). Patent, on the other hand, is a combined technological solution, which partially or completely is accomplished through using a computer program. The EU Directive 2009/24/EC requires Member States to accord protection to computer programs under copyright law as literary works (Council of European Union, 2009, pp. 16–22). Copyright covers the protection of both object and source code from verbatim copying (Karjala, 1998, p. 525). Commonly, the length of copyright protection in the EU is the author's life plus 70 years, or 70 years after the work is lawfully made available to the public, and in terms of related rights for 50 years after the event which set the term running (Council of European Union, 2006, pp. 12–18).

Copyrights are moral and economic rights. The main economic rights are the right to reproduction, the right to communicate the work to the public, and

the right to make adaptations. Moral rights are inseparable from the author and safeguard author's right to authorship and his reputation (WIPO, 2015a). The right holder of a computer program may authorise or do the translation, adaptation, arrangement and any other alteration of the program, permanent or temporary reproduction of the program or a part thereof and distribution of the program (Council of European Union, 2009, Art. 4). The author of a computer program is a natural person(s) or a legal person if the legislation of the Member State permits (Council of European Union, 2009, Art. 4, Para. 1). In case an employee creates a computer program in the execution of his duties or following the instructions given by the employer, the economic rights of the author are transferred to employer if the employment contract does not provide otherwise (Council of European Union, 2009, Art. 4, Para. 3).

Often the protection to computer programs is sought in combination of different legal and technical means including copyright, trade secret, patents and licence contracts.

One way to regulate the export of a technology is through licensing. Licences usually involve the purchase of production or distribution rights and knowhow (Maskus, 2004, p. 1). Licences are not a form of intellectual property rights but means that regulate how licensees can use the work and related intellectual property rights while licensors retain the IP ownership.

Based on accessibility to source code, software can be categorised as closed or open source. A product can be licensed by both closed source and open source licences. In a closed source software model the creators adhere the source code and license or sell the object code of the program to the software users (Michler, 2005, p. 262). Open source software model provides users with a greater freedom as the source code is freely distributed and users can use, copy, modify and redistribute it, but it is licensed with restrictions and typically the users are asked to make the source code widely available and license the changed software under the same terms which the original licence was granted (Michler, 2005, p. 262). It should be brought out that when a party who outsources the software by claiming exclusive rights to the software, therefore precluding reuse of the source code, it means that the developer would have to start from scratch each time a new software package is developed for a different party (Horne, 1992, p. 499).

Regarding software developed for the state, the issue who is the owner of the rights varies from country to country and is based on national laws and policies. It can be affected also by the national public procurement law if it stipulates concrete requirements in regard with outsourcing IT developments.

4. International technology transfer

Commonly it is more difficult for less developed countries to innovate technologies than to obtain these from developed countries where technical modernising has taken centuries (Michaels, 2009, p. 231). International technology transfer occurs between any two countries and is not only focused on less developed countries. "International technology transfer refers to any process by which a party in one country gains access to the technology of another party in a second country and successfully learns how to absorb it into its production function" (Michaels, 2009, p. 231).

Technology transfer is affected by taxation policies, free trade agreements, export policies, state interests and other factors. Legal, political, regulatory and social factors vary from country to country and have direct effect on technology transfer. Even more these factors come under the question if the subject is strategical to the country.

Strategic ICT solutions can be used in public circulation or not. The abovementioned ID card system is strategic as it is important for the state due to the wide range of usage and importance. The ID card system is being used by private persons and private sector as well as the state to offer services. On the other hand, military technologies are strategical and out of public use. Countries do not want so much the products of technology but the licence of the technology in order to manufacture the products on their own (Levine, 1986, p. 373). There needs to be a balance between the needs of recipients of the military technology, private sector producers and the country's military posture but it should be kept in mind that having a technological leadership over some specific countries can be a cornerstone of the transferring country's military strategy. That leadership was achieved by US in the 1980s by restricting the transfer of technology. (Levine, 1986, p. 375)

It is under national discretion and laws to who and on what conditions the countries' strategic and critical IT developments are to be exported. Article 66, Paragraph 2 and Article 67 of TRIPS Agreement stipulates the obligation of the developed countries to provide positive incentives for international technology transfer to the least-developed countries and obligates the developed countries to provide technical and financial cooperation in favour of developing and least-developed countries to help induce more international technology transfer (TRIPS, 1994, Art. 66, Para. 2; Art. 67). Yet in practice even if the governments of developed countries would be willing to offer substantial incentives they

would face domestic political opposition and therefore many decisions are made based on political reasons (Maskus, 2004, p. 3). Therefore international technology transfer combines in itself intellectual property rights together with trading and public policy matters. One example regarding international technology licensing can be given about Latin America, where in the 1970s they drafted specialised technology transfer laws with the intention of regulating the content of technology licensing agreements and ensuring that the development objectives of a host country economy would not be undermined by unequal terms in technology transfer transactions (UNCTAD, 2001, p. 17).

5. Military technology transfer agreements

Technology transfer of military technology has been around longer than the export of state-owned ICT solutions. Countries that have not been active in military technology transfer can learn from this field. On the other hand, in some countries, like the US, there are policies and laws conducted to govern the technology transfer in general and therefore the same applies to the export of strategically important ICT solutions.

Technology transfer in the US is regulated by numerous US government agencies and is in due course controlled through a government-to-government agreement that can take the form of a memorandum of understanding, general security agreement, letter of offer and acceptance, export licence, or other form agreed to by both governments (DISAM, 2015, Ch. 7). The main policy governing the course of technology transfer is included in Department of Defence (DoD) Directive regarding international transfers of technology, goods, services, and munitions and applies to all technology transfer mechanisms. According to that Directive, among others, transfers of technology must be in line with US foreign policy and national security objectives, limit the transfer to any other country that support specific national security or foreign policy objectives, share military technology only with allies and other nations that cooperate effectively, provide special attention to rapidly emerging and changing technologies to protect against the possibility that the technology might be conveyed to potential adversaries before adequate safeguards can be implemented and strive, before transferring valuable defence-related technology, to ensure that such technology is shared reciprocally (DoD, 1984). The control over export of software and technologies in general is necessary to evaluate the ultimate destination country, the control and the intended end-

use to see if the product is capable of being used as determined by the US government (Carrier, 2011, p. 11).

Among other things, data exchange agreements, including licensing, co-development and coproduction agreements, patents and sales to third-party nations are used to affect transfers (DISAM, 2015, pp. 7-3, 7-4). Before transaction can take place security-related conditions must be met—the recipient country agrees not to transfer the export subject to anyone who is not an officer, employee or agent of the country and not to use the export subject or permit its use for other than the purpose for which they were furnished without prior consent of US government, the recipient country agrees to preserve security and provide substantially the same degree of security as the US (DISAM, 2015, p. 7-5).

The US model has been criticised because it does not have a single agency as supervisor to control licensing and enforcement (DISAM, 2015, p. 7-5).

As strategically significant technology export can undermine national security, respective authority has to issue a licence before any dual-use technology transfer takes place to a potential adversary (US Dept. of State Dispatch, 1993, p. 19). National licensing system is a primary tool in export control (Hsu, 2010, p. 706). US Army Research Laboratory is authorised to license its intellectual property and these Patent Licence Agreements can be: exclusive, by restricting the use of an invention to a single licensee; partially exclusive, by allowing multiple licensees but restricting the use of the invention by any single licensee to a particular geographic area or use; and non-exclusive by allowing to issue licence to any number of licensees (US Army Research Laboratory, 2010).

The problems that the US have had may be the same or refer to the problems that may arise with the export of strategically important ICT solutions. One of the issues in 1990 was the security situation in the recipient countries, their intentions and their communication with Soviet intelligence agencies and the effect of export of technologies to US commercial competitiveness (Benson, 1990, p. 19). Although nowadays the situation is different, these decisions are still affected by politics and the situation in the recipient country. In March 2015, Sweden announced that they will cancel a ten-year military cooperation agreement with Saudi Arabia after criticism of Riyadh's human rights record sparked a diplomatic row (Duxbury, 2015). The decision was made by Swedish Social Democrat-led government whose focus in foreign policy is on human rights. The decision was criticised by more than 30 business executives as they saw that this shove would jeopardise Sweden's reputation as a trade and cooperation partner (*Newsweek*,

2015). Likewise there were recommendations made to speed the export control process by which it was determined if the transfer is in line with US policy and make it less complicated (Benson, 1990, p. 21).

As US government is strict regarding permitting its military technology to be passed on to other countries, it has affected also exports of European companies that use US technology in their products (Hoyos, 2013). Therefore, even if the recipient countries' policies are less stringent then the source countries' policies can still affect technology transfers. It is brought out that sharing technology with foreign governments is becoming more and more important with the aim of winning big defence deals (Hoyos, 2013).

6. Estonian legislative environment regarding exporting e-services

Before analysing the opportunities and obstacles in regard with exporting e-services, it should be pointed out how the public sector in Estonia obtains the software.

In order to develop and obtain software for e-services the public sector usually announces procurement. The reason mostly relies on the fact that the public sector does not have officials in its service to develop or create software for e-services. Therefore, in order to ensure the effectiveness, reliability and constant developing of the e-services and therefore also cost savings, the public sector subscribes these services from private sector.

Public Procurement Act is the legal instrument that stipulates the rights and obligations of subjects involved in order to grant the effectiveness and legality of public procurement. There are two options based on the law to organise public procurement for a software:

1) Contracting for services through public contract. Public contract is a contract which has been awarded to one or multiple persons by contracting authority or authorities as a result of public procurement, establishes mutual material obligations and the objects of which are services, public works or supplies (Public Procurement Act, 2007, Art. 4, Para. 1); and
2) organising design contest to have proprietary rights and user rights of a software which can lead to awarding a public service contract. Design contest refers to procedure that allows public authority to obtain a plan or design selected by a jury in the course of a competition mainly in the fields of architecture, planning, information systems, engineering works,

> software development or data processing. (Public Procurement Act, 2007, Art. 9, Para. 2)

In practice, regardless of these two options provided in the law, other procurement procedures are used in order to obtain software (Rosentau, 2008, p. 23). For example, Paragraph 6[1] on public-private partnership and Paragraph 8 on dynamic purchasing system procurement procedures can be used as it is difficult to explain why it should be forbidden or excluded although the law does not precisely allow it (Rosentau, 2008, p. 23). In regard to IT procurements, the Copyright Act and Law of Obligations Act should be applied to procurement contract. It means that a procurement contract has to conform to the requirements of author's contract set forth in the Copyright Act and provisions regarding licence contracts in the Law of Obligations Act.

The policy and practice of IT procurements have to fulfil the principles of the free dissemination of ideas and information, sustainability, innovation and free competition. If the competing entities are on equal terms, then the one who is offering a solution by providing open source code, has less requirements for protecting trade secret and is willing to assign all proprietary rights will win the procurement. (Rosentau, 2008, p. 3)

There are four ways how the state develops e-services: the state obtains all proprietary rights of the e-service; it obtains part of proprietary rights of the e-service; it obtains user licence without obtaining copyright; and it uses e-service on service-based terms (Rosentau, 2008, p. 4). Providing that the state develops e-service in a latter way, it will not obtain the licence of the software nor proprietary rights of the copyright. The state obtains part of proprietary rights of the e-service, for example, in a case where a third person's software or database is used. In Estonia, the state can transfer a state-owned ICT system through open source or closed source licence or international agreement.

In the event where the state owns proprietary rights of the e-service, as software can be financially assessed, it is a part of state assets. Due to the fact that software is an intangible asset it is possible that the same software is used at the same time by other users. Therefore licensing would not constitute an obstacle in practice. The actions which can be done with state assets and how are provided in the State Assets Act. Paragraph 1 of Article 15 of the State Assets Act stipulates that authorisation to use state assets may not be granted where the assets are required for the purpose of exercising state authority or for any other public purpose or where authorising the use of the assets by another significantly impairs the intended use of the assets or renders it impossible. However, an

exception can be made as it is stated in the State Assets Act (2009, Art. 2, Para. 5) that the provisions of that act will not apply to the transfer of state assets into the use or ownership of a foreign state provided government delegations or other competent institutions have decided so in writing. It is also brought out that only with the consent of the Government of the Republic of Estonia, a minister or State Secretary may decide to grant authorisation to use the property, when the value of the movable property exceeds one million euros or the term to use exceeds one year (State Assets Act, 2009, Art. 19, Para. 3).

The current system raises a question of its effectiveness. The state has set down the principles that the subject of outsourcing has to own all the copyrights and exclusive licence regarding the product, therefore the existing solutions cannot be applied. That leads to the question of whether the system is cost-effective and meets the requirements of Article 1 of the Public Procurement Act which stipulates the requirement of transparent, purposeful and economical use of the financial resources of the contracting authority. The state should license the solution back to the private sector in order to meet the requirement of the abovementioned provision and gain more from the private sector competence. Currently, the strongest emphasis goes to the quality of product but not to the variety of service providers which can lead to infringement of EU competition law. Regarding strategically important ICT solutions having one secure partner as well as granting safety is in the interests of the state and public. Paragraph 1 of Article 15 of the State Assets Act constitutes an obstacle to transferring state-owned ICT solutions and should not be applicable to ICT solutions. It should also be stated in the law that state assets can be transferred through open source licence, though currently there is no such provision and in order to export X-Road via EUPL it was brought out in the regulation about X-Road. There has not been discussion regarding who should make the decision and whether the current process covers the needs. Whether the ICT solution should be transferred or not could be decided by centralised regulatory agency or by a government. As it is stipulated that only when the value of the movable property exceeds one million euros, then with the consent of the Government of the Republic of Estonia a minister or State Secretary may decide to grant authorisation to use the property, there emerges a question of how to act in a situation where it is hard or impossible to derive the value. Software is immaterial and therefore the question of how to determine the value is not clear.

It was concluded in the research regarding measuring the impact of e-services that the main obstacle for exporting e-services is the fact that the legal and organisational environment varies in different countries and thus the main Estonian e-services would not have a place in the global market (Kalvet, Tiits

& Hinsberg, 2013). Another obstacle has been the lack of research about social and economic benefits of e-services which has made it difficult to explain the benefits and demonstrate the effects of e-services. It was pointed out in the research that in order to develop the export of e-services, Estonian ICT solutions, such as the ID card and digital signature system, should have international compatibility. The e-services are largely connected with Estonian public sectors' institutional management or the Estonian legal system. The research outlined that most e-services were quite easy to copy and the most innovative solutions were e-voting, X-Road, and the functionality of the ID card.

7. Exporting X-Road: the Estonian example

Technology licensing and transfer of technology are important features in international joint ventures and strategic alliances with the purpose of maintaining a competitive edge in a market economy (WIPO, 2015b). Estonia has had the experience of transferring ICT solutions to other EU and non-EU countries. By transferring the X-Road and Judicial Information System, the government is also expecting to benefit from it. For instance, sharing the costs of development with recipient country reduces the costs of developing for Estonia.

The Judicial Information System (*Kohtute infosüsteem*), which was outsourced by Estonian state and operates under the Ministry of Justice, was established in 2006. It is a database under the State Information System and its goal is to organise the work of the courts, systematising and making available the court decisions and collect statistics on court decisions (RIHA, 2015). The Judicial Information System has consolidated the court cases into one single database, processes the data of procedural steps and the electronic documents, thus granting ongoing overview of judicial proceedings and enabling analysing of courts' workload and rulings (RIHA, 2015). The system has simplified the work of many and it is being further developed by Estonian IT companies in other countries, for example in Iraq. However, it may be questionable whether the Judicial Information System is strategically and critically important to the state but X-Road certainly is.

Before Estonia started exporting the X-Road, the Government of the Republic of Estonia issued a regulation 'Data exchange layer of information systems' (2008; *Infosüsteemide andmevahetuskiht*), which stated that European Union Public Licence (EUPL) will be the official licence to distribute X-Road. Elaboration of a European open-source licence, EUPL, started in 2004 by European Commission

(Dusollier, 2007, p. 1429). It was brought out in the Preamble of EUPL that its purpose is to promote interoperable delivery of European e-Government service to public administrations, businesses and citizens advancing therefore the use and distribution of state-owned ICT solutions inside the EU. Through EUPL, licensor gives licensee a world-wide, non-exclusive, royalty-free, sub-licensable licence to use, reproduce, modify, distribute, communicate to the public, lend and rent the work. EUPL was used to provide documentation, knowhow and source code of the X-Road to Finland.

Estonian Prime Minister has said that the cooperation between Estonia and Finland has been very good for years and, taking into account the global post crisis economic situation, Estonia and Finland should have even more cooperation to strengthen both countries' economies and to find new markets for export (Lakson, 2015). On 10 December 2013, Andrus Ansip, the then Prime Minister of the Republic of Estonia, and Jyrki Katainen, the Prime Minister of the Republic of Finland, digitally signed the Memorandum of Understanding to affirm cooperation in the field of information and communication technologies regarding X-Road and e-data interchange (Estonian Ministry of Foreign Affairs, 2014; Cybernetica, 2014). It was the first known digitally signed international agreement between governments. The Memorandum stipulated that Estonia and Finland will further develop together the X-Road, which is in use in Estonia, in order to have cross-border e-services. On 18 November 2014 Estonian Prime Minister, Taavi Rõivas said at the biggest international event of regional start-ups, investors and technology that Estonia and Finland are the first countries in the world to nationally unite their e-services and create a single digital economic space (Government of the Republic of Estonia, 2014).

X-Road is a decentralised environment which enables public and private e-service databases to connect, integrate and work together. It is the backbone of the Estonian e-government, has operated for more than 12 years with more than 2,000 e-services and over 900 organisations, public registers and databases are connected to the environment (Cybernetica, 2013). "The X-Road system uses the concept of digital signatures and contains its own Public Key Infrastructure (PKI) that guarantees confidentiality, integrity and traceability of the exchanged data." (Cybernetica, 2015) It means that the location or ownership of the data will not be altered, and the registers and databases will not be centralised (Cybernetica, 2013, p. 5). The data will be managed by the same institutions that should manage them anyway. The need to develop this kind of environment emerged from the fact that when the state databases were in the growth stage, there was no central platform and therefore the databases were cross-used (RIA, 2015a). It should be pointed out that every e-solution that has to use several

databases use X-Road. Many successful e-services have been built by using the X-Road functions (e.g., applying for family allowance, public examination results service) and many databases have joined X-Road in order to use its practicality (e.g., the Judicial Information System). Its success derives from the fact that each year the number of inquiries made is rising—in 2013 more than 287 million inquiries were made (RIA, 2015a). Also, an "e-police" program used in police cars communicates via X-Road with necessary databases, such as traffic, criminal record, gun and civil registry. That has proved to make police work more efficient, quicker and safer (RIA, 2015b). Private users can make inquiries and check information regarding them via X-Road.

Finland receives guidance from the Estonian Information System's Authority and is building a decentralised environment similar to Estonian X-Road (E-Estonia, 2013). The cooperation is based on the current version of X-Road and its source code. The purpose of the cooperation is to understand the organisation and agreements that create the frameworks for X-Road technology (Estonian Public Broadcasting Agency, 2013). Owing to the ID card software, which supports both Estonian and Finnish ID cards, Finnish and Estonian authorities can exchange information, persons can exchange documents and conclude contracts by using the digital signatures mutually (*ID.ee*, 2013). The benefit of exporting X-Road to Finland lies in bilateral cross-border e-services and the fact that enterprises and citizens can submit information just once. It was said that in Finland X-Road will be put into practice in spring 2015 and therefore all the necessary bases for cross-border cooperation are created (E-Estonia, 2015). It has been recommended that Estonia and Finland should establish a shared governance mechanism for cross-border services and data exchange as well as joint infrastructure management such as digital signatures, interoperability layers or electronic identities in order to provide basis for future expansion of cross-border services (OECD, 2015, p. 50). At present, negotiations regarding developing and agreeing on a more precise road map for development of cross-border data exchange and services are being held (Estonian Embassy in Helsinki, 2015).

Nevertheless, X-Road has not only been exported to Finland, but also to Azerbaijan as they have had a boom in e-infrastructure and electronic government services. Azerbaijan's president pushed for the digitisation of state services and Estonian companies responded to the call. They implemented mobile ID, a number of e-government projects as well as installed an "updated" version of X-Road. As it was more secure and efficient to use a centralised mobile ID platform, offered as a service to the telecom providers, than the Estonian model, where service platform is owned by three telecoms, then Estonia has decided to implement the same kind of arrangement. (E-Estonia, 2014)

8. Conclusion

It is clear that every EU country has its own policies regarding technology transfer, ownership of state e-services and the possibilities how the state-owned or licensed e-service could be exported. However, not only the interests of contracting parties but also the countries' national interests should be taken into account. The obstacles to technology transfer should not be political in nature and priorities have to be rearranged in favour of long-term objectives (Hamza & Stovall, 1987, p. 5). Transfers of technology must be in line with foreign policy as well as national security purposes.

Government cooperation with only one service provider can raise questions regarding competition laws. A better solution would be to set down in the law how state-owned ICT solutions can be distributed, other than making separate laws regarding each ICT solution. If the provisions regarding technology transfer are in connection with a certain amount of money, it could pose a threat to export as software is immaterial and the question how to determine its value is not clear.

Establishment of a centralised regulatory agency who would control licensing, coordinate primary enforcement, develop model contracts, cooperate with public and private sector entities in technology export negotiations and be the central point for transactions regarding technology transfer agreements seems to be one way of dealing with things. It would be a good option for the countries who have to carry out many critical and strategic technology transfers in a year (e.g., Sweden). Currently, not many state-owned strategic IT technology transfers take place and therefore the decisions are mostly made on a case-by-case basis and via bilateral agreements.

Digital cooperation between countries strengthens the economy of both countries and enables them to find new export markets. Therefore, legal provisions which are outdated and therefore impede technological cooperation and IT solutions export should be revised. The ownership of intellectual property might pose a threat to technology transfer or further development of the IT solution.

As in military technology transfer, so in the export of strategically important IT solutions, trust between the parties and the situation in the countries play important roles. The agreement between Estonia and Finland would not have been concluded had there not been trust between these two countries concerning online security (European Commission, 2014). Based on China's experience, several restrictions on foreign-related technology transfer, such as, for example,

inadequate intellectual property enforcement, burdensome prior approval and registration requirements for importing and exporting technology, expressively discourages cross-border technology export (Sun, 2003, p. 22).

As inside the EU the countries do not have as marked differences between each other, the developed IT solution most probably would work in other Member States as well. This example can be illustrated by the Estonian-Finnish cooperation. Working relations between Estonia and Finland have to integrate governance lessons learnt both domestically and at the EU level (OECD, 2015, p. 255). The experience can be expanded to cover further EU Member States. Taking into account the free of movement of goods, the EU has created a platform to cooperate and export IT solutions. However, the lack of preparedness of infrastructures, legislation and stakeholders for cross-border exchanges poses a threat to IT transfer and should be taken into consideration in the EU as well. As there are differences between digital developments inside the EU, especially in the Digital Public Services area, the more developed EU Member States could be beneficial to all parties by exporting to or furthering development and cooperating with destination country. Strong collaboration would enable mutual learning from past experiences along with the opportunities for better use of technology.

Further research in the field of transferring strategically important IT solutions is needed. It is necessary to analyse whether the states' practice of using certain IT companies is infringing EU competition law, or is the current practice justified based on reasons of public interest. Additionally, analyses are needed in the field of IP rights—that is, what are the legal consequences for the state if an IT solution in question has many right-holders. Legal problems raised in the case of Estonia serves as a useful example for other countries.

Anni Säär works as a legal expert at the Estonian Human Rights Centre since 2011, representing Estonia in EU Civil Society Platform against Trafficking in Human Beings. She is pursuing a Master of Arts degree in Law and Technology at the Tallinn University of Technology, where she has been teaching a course on the Rights, Obligations and Liability of Users on the Internet. Anni Säär is involved in the research on AI and systematisation of legal norms.

Addi Rull works as lecturer at the Tallinn Law School of Tallinn University of Technology since 2010. He coordinates the master's programme in Law and Technology and teaches several IP and IT law courses. He is working towards PhD degree in informatics, researching the field of AI and systematisation of legal norms. Before joining the Law School, Addi Rull worked in the business sector and completed LLM degrees in European Intellectual Property Law and Law and IT from Stockholm University.

References

Apple Computer, Inc. v. Franklin Computer Corporation [1983], US Court of Appeals Third Circuit, 30.08.1983, 714 F.2d 1240, 219 USPQ 113.

Benson, S. (1990), 'The technology transfer dimensions of U.S. military assistance,' *The DISAM Journal*, pp. 18–22.

Canfield, J. (1984), 'Copyrightability of object code,' *Notre Dame Law Review*, vol. 59, no. 2, p. 412–430.

Carrier, M. K. (2011), 'Introduction to U.S. export control: regulations for patent practitioners,' *Akron Intellectual Property Journal*, vol. 5, no. 1, pp. 1–17.

Council of the European Union (2006), Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights, *Official Journal of the European Union*, OJ L 372, 27.12.2006.

—— (2009), Directive 2009/24/EC of the European Parliament and of the Council of 23 April 2009 on the legal Protection of computer programs, *Official Journal of the European Union*, OJ L 111, 5.5.2009.

—— (2015), *Digital Economy and Society Index 2015: Methodological note*, Brussels: European Commission Directorate-General for Communications Networks, Content and Technology.

Curtis, S. & Hoggins, T. (2014), 'Is Destiny the most expensive video game ever made?' *The Telegraph*, 9 September 2014.

Cybernetica (2013), 'X-Road eGovernment Interoperability Framework (X-Road whitepaper).' Retrieved from http://cyber.ee/uploads/2013/03/cyber_xroad_NEW2_A4_web.pdf [accessed 2 Jul 2015]

—— (2014), 'X-Road reaches Finland'. Retrieved from http://cyber.ee/en/news/x-road-reaches-finland/ [accessed 1 Jul 2015]

—— (2015), 'X-Road'. Retrieved from http://cyber.ee/en/e-government/x-road/ [accessed 2 Jul 2015]

Data exchange layer of information systems (2008), 'Infosüsteemide andmevahetuskiht,' *Riigi Teataja*, RT I 2008, 18, 129.

DISAM (2015), *The Management of Security Cooperation (Green Book)*, 34th edition, Wright-Patterson AFB, OH: Defense Institute of Security Assistance Management.

DoD (1984), *International Transfers of Technology, Goods, Services, and Munitions*, Department of Defense Directive Number 2040.2, 17.1.1984.

Dunning, J. H. (2013), *Multinationals, Technology & Competitiveness*, Routledge Library Editions: International Business, vol. 13, Abingdon: Routledge.

Durell, K. L. (2000), 'Intellectual property protection for computer software: how much and what form is effective?' *International Journal of Law and Information Technology*, vol. 8, no. 3, pp. 231–262.

Dusollier, S. (2007), 'Sharing access to intellectual property through private ordering,' *Chicago-Kent Law Review*, vol. 82, no. 3, pp. 1391–1435.

Duxbury, C. (2015), 'Sweden ends military cooperation deal with Saudi Arabia: criticism of Saudi rights record causes diplomatic standoff,' *The Wall Street Journal*, 10 March 2015.

E-Estonia (n.d., a), 'Electronic ID Card.' Retrieved from https://e-estonia.com/component/electronic-id-card/ [accessed 2 Jul 2015]

—— (n.d., b), 'E-Prescription.' Retrieved from https://e-estonia.com/component/e-prescription/ [accessed 1 Jul 2015]

—— (2013), 'Top 5 Technology Transfers from e-Estonia.' Retrieved from https://e-estonia.com/top-5-technology-transfers-e-estonia/ [accessed 5 Jul 2015]

—— (2014), "Estonia's Digital Revolution Takes Root in Azerbaijan," 13 August 2014. Retrieved from https://e-estonia.com/estonias-digital-revolution-takes-root-azerbaijan/ [accessed 4 Jul 2015]

—— (2015), 'Estonia and Finland to plug in Real-Time Economy,' 14 January 2015. Retrieved from https://e-estonia.com/estonia-and-finland-to-plug-in-real-time-economy/ [accessed 4 Jul 2015]

E-Governance Academy (n.d.), 'Change Management (CHARE)'. Retrieved from http://www.ega.ee/domains/central-e-government/change-management-chare/ [accessed 1 Jul 2015]

Estonian Embassy in Helsinki (2015), 'Relations,' 2 June 2015. Retrieved from http://www.estemb.fi/eng/estonia_and_finland [accessed 4 Jul 2015]

Estonian Ministry of Foreign Affairs (2014), 'Eesti ja Soome: Kahepoolsed Suhted'. Retrieved from https://peaveeb.vm.ee/?q=en/node/143 [accessed 29 Jun 2015]

Estonian Public Broadcasting Agency (2013), 'Finland to set up its own data X-Road, cross-border e-services in the works,' 13 September 2013. Retrieved from http://news.err.ee/v/scitech/89928bc5-f5df-407d-9dbd-3f4a97e80e8a [accessed 4 Jul 2015]

European Commission (2014), 'The Digital Single Market – investing in the future,' Speech by Vice-President Andrus Ansip on 11 December 2014 at the LIKTA 16th Annual Conference in Riga, European Commission.

Frankel, M. J. (2012), 'Secret sabermetrics: trade secret protection in the baseball analytics field,' *Albany Government Law Review*, vol. 5, no. 1, pp. 240–284.

Government of the Republic of Estonia (2014), 'Peaminister Rõivas Slushil Helsinkis: ehitame e-residentsusest järgmise eduloo' [Prime Minister Rõivas attending Slush in Helsinki: e-residency will be our next success story]. Retrieved from https://valitsus.ee/et/uudised/peaminister-roivas-slushil-helsinkis-ehitame-e-residentsusest-jargmise-eduloo [accessed 1 Jul 2015]

Hamza, S. M. & Stovall, H. L. (1987), 'Proposed law to regulate technology transfers in Egypt,' *Arab Law Quarterly*, vol. 2, no. 1, pp. 3–11.

Horne, A. J. (1992), 'Shared rights to source code: the copyright dilemma,' *Santa Clara Law Review*, vol. 32, no. 2, pp. 497–538.

Hoyos, C. (2013), 'Europe defence groups urge technology sharing,' *The Financial Times*, 13 October 2013.

Hsu, L. (2010), '2000–2009: A decade of security-related developments in trade and investment,' *Journal of World Investment & Trade*, vol. 11, no. 5, pp. 697–729.

IBM (1998), European Patent Office T 1173/97.

ID.ee (2013), 'Estonian and Finnish Prime Ministers signed the ICT Memorandum of Understanding digitally,' 11 December 2013. Retrieved from http://id.ee/index.php?id=36546 [accessed 4 Jul 2015]

Kalvet, T.; Tiits, M. & Hinsberg, H. (2013), *E-teenuste kasutamise tulemuslikkus ja mõju* [Efficiency and effect of e-service usage], Tallinn: Balti Uuringute Instituut ja Poliitikauuringute Keskus Praxis.

Karjala, D. S. (1998), 'Copyright protection of computer program structure,' *Brooklyn Law Review*, vol. 64, no. 2, pp. 519–543.

Lakson, P. (2015), 'Taavi Rõivas Helsingis: Soome on Eesti olulisim partner' [Taavi Rõivas in Helsinki: Finland is Estonia's main partner], *Postimees*, 14 April 2015.

Levine, H. (1986), 'Technology transfer: export controls versus free trade,' *Texas International Law Journal*, vol. 21, no. 2.

Lin, D.; Sag, M. & Laurie, R. S. (2002), 'Source code versus object code: patent implications for the open source community,' *Santa Clara Computer and High Technology Law Journal*, vol. 18, no. 2, pp. 235–257.

Ma, Z. (2010), 'On relationship between technology standards and patented technology licensing,' *Journal of Politics and Law*, vol. 3, no. 1, pp. 16–23.

Maskus, K. E. (2004), *Encouraging International Technology Transfer*, UNCTAD-ICTSD Project on Intellectual Property Rights and Sustainable Development, Issue Paper no. 7.

Michaels, A. (2009), 'International technology transfer and TRIPS Article 66.2: Can global administrative law help least developed countries get what they bargained for,' *Georgetown Journal of International Law*, vol. 41, no. 1, pp. 223–261.

Michler, C. (2005), "The procurement decision – 'open' or 'closed' source software?" *Deakin Law Review*, vol. 10, no. 1, pp. 261–269.

Newsweek (2015), "Sweden's odd military alliance with Saudi Arabia," 9 March 2015.

OECD (2015), *OECD Public Governance Reviews: Estonia and Finland: Fostering Strategic Capacity across Governments and Digital Services across Borders*, Paris: OECD Publishing.

Population Register (n.d.), [*Rahvastikuregister*], Ministry of Interior Affairs. Retrieved from https://www.siseministeerium.ee/et/tegevusvaldkonnad/rahvastikutoimingud/rahvastikuregister [accessed 6 Jul 2015]

Public Procurement Act (2007), 'Riigihangete seadus,' *Riigi Teataja*, RT I 2007, 15, 76, 24.

RIA (2015a), 'Eesti IT edulood' [Estonian IT success stories], *Riigi infosüsteemi teejuht*. Retrieved from https://www.ria.ee/teejuht/eesti-it-edulood [accessed 2 Jul 2015]

—— (2015b), 'Kogu riigi infosüsteem ühes autos' [A whole country's information system in a single car], *Riigi infosüsteemi teejuht*. Retrieved from https://www.ria.ee/teejuht/eesti-it-edulood/kogu-riigi-infosusteem-uhes-autos [accessed 30 Jun 2015]

RIHA (2015), *Riigi infosüsteemi haldussüsteem, Infosüsteem: Kohtute infosüsteem* [The State Information System, Information System: Judicial Information System]. Retrieved from https://riha.eesti.ee/riha/main/inf/kohtute_infosusteem [accessed 1 Jul 2015]

Rosentau, M. (2008), 'Riigi ja kohaliku omavalitsuse asutuste poolt tellitava arvutitarkvara autoriõiguste omandamise, litsenseerimise ja teenusepõhise kasutuse põhimõtted' [Principles of acquiring, licensing and service-based use of copyrights of computer software procured by state and local government offices], Version 1.0/20.11.2008.

Rowe, E. A. (2009), 'Contributory negligence, technology, and trade secrets,' *George Mason Law Review*, vol. 17, no. 1, pp. 1–37.

Rull, A.; Täks, E. & Norta, A. (2014), 'Towards software-agent enhanced privacy protection,' in T. Kerikmäe (ed.) *Regulating eTechnologies in the European Union*, Cham, etc.: Springer, pp. 75–77.

Ryanair Ltd v PR Avaiation BV [2015], CJEU, Case C-30/14, ECLI:EU:C:2015:10.

Scott, M. D. (2006), *Scott on Information Technology Law*, 3rd ed., Aspen Publishers: Wolters Kluwer Law & Business.

Sepp, O. (1999), 'Rakendusjuhised ID-kaardi pilootprojektide läbiviimiseks' [Application guide for carrying out ID card pilot projects], *Cybernetica*. Retrieved from http://www.id.ee/public/rakendusjuhised.pdf [accessed 2 Jul 2015]

Stephens, K. P. & Sumner, J. P. (1996), 'Software objects: a new trend in programming and software patents,' *Santa Clara Computer and High Technology Law Journal*, vol. 12, no. 1, pp. 1–30.

Szattler, E. (2007), 'Patentability of computer programs,' *Masaryk University Journal of Law and Technology*, vol. 1, no. 1, pp. 97–108.

State Assets Act (2009), 'Riigivaraseadus,' *Riigi Teataja*, RT I 2009, 57, 381.

Sun, C. (2003), 'Technology import and export in post-WTO China,' *IPL Newsletter*, vol. 21, no. 4.

TRIPS (1994), TRIPS: Agreement on Trade-Related Aspects of Intellectual Property Rights, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, The Legal Texts: the Results of the Uruguay Round of Multilateral Trade Negotiations 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197.

UNCTAD (2001), *Transfer of Technology*, United Nations Conference on Trade and Development, UNCTAD Series on issues in international investment agreements.

US Army Research Laboratory (2010), 'Patent Licensing.' Retrieved from http://www.arl.army.mil/www/default.cfm?page=15 [accessed 28 Jun 2015]

US Dept. of State Dispatch (1993), *Fact Sheet: U.S. Export – Strategic Technology Controls*, US Department of State Dispatch Supplement, August 1993, vol. 4, no. 3.

Vedinas, V. (2012), 'Aspects of the privatization of public services,' *Juridical Tribune*, vol. 2, no. 2, pp. 6–12.

Vicom (1986), European Patent Office T 0208/84.

Villapaz, L. (2013), "'GTA 5' costs $265 million to develop and market, making it the most expensive video game ever produced: Report," *International Business Times*, 8 September 2013.

WIPO (2015a), 'Copyright,' World Intellectual Property Organization. Retrieved from http://www.wipo.int/copyright/en/ [accessed 27 Jun 2015]

—— (2015b), 'Licensing and Technology Transfer,' World International Property Organization. Retrieved from http://www.wipo.int/patent-law/en/developments/licensing.html [accessed 29 Jun 2015]