ments often advanced in favour of declassifying certain illegal drugs so that these may be better controlled, since borrowing again from the late 1980s, "... the beat of Sergeant Pepper and the soaring sounds of the Miserere from unlawful copies are more powerful than law-abiding instincts or twinges of conscience".[63]

Lastly, it may nonetheless conversely be remarked, leaving aside such arguments and returning somewhat fittingly in closing to Templeman LJ's observation in *Amstrad,* that whereas in 1988 "copyright law could not envisage and ... cope with mass production techniques and inventions which create a vast market for works of the copyright owner but also provide opportunities for his rights to be infringed"[64], the DMCA safe harbour provisions, as passed in a democratic process, were intended to address precisely such problems. The question therefore remains whether and to what extent Stanton J's item specific knowledge standard follows the law as it now stands, or whether it smacks of judicial activism. Whilst the above discussion has aimed to provide different perspectives, this question begs further extensive discussion in its own right. In this regard, whilst some readers will undoubtedly anticipate Viacom's appeal with eagerness others will do so with trepidation. Whatever the particular predilection or sentiment it is likely that an appeal, given the importance of this case to this area of law, will be of more than passing interest.

63 For an interesting comment which despite originating in 1988, supports such a line of argument, see *Amstrad* (n 2), 1060.

64 *Ibid.*

Thomas Hoeren

IMMI – The EU Perspective

On June 16th 2010, the Icelandic Parliament unanimously passed a proposal tasking the government to introduce a new legislative regime to protect and strengthen modern freedom of expression, and the free flow of information in Iceland and around the world (see www.immi.is). The idea is to collect the most liberal media acts in the world and transform their concepts into a new Icelandic media act so that Iceland becomes an attractive environment for the registration and operation of international press organizations, human rights groups (such as Wikileaks) and internet data centers. The concept proposed is fascinating as it shows visions for a new European media regulation regarding internet journalism. However, this proposal cannot be seen only from the Icelandic point of view. As Iceland is not only a member of the European Economic Area (EEA) but also applying for full EU-membership (www.eeas.europa.eu /iceland/index_en.htm– last visited 10-08-2010), it is essential to consider the European perspective before such a legislative package can be successfully drafted.

Most importantly, the article therefore takes a closer look at the topics of data retention (I.), liability (II.), process protection (III.), the publication rule regarding archives (IV.) and whistleblower's protection (V.).

I. Data Retention

According to the Icelandic telecommunications law no. 81/2003 Iceland's telecommunication providers are obliged to keep records of all connection data for 6 months[1]. The reason for this law being into effect is the EU Directive 2006/24/EC which requires data retention for not less than six months[2]. However, this topic is still under vital discussion.

On 2 March 2010, the German Constitutional Court declared German data retention laws unconstitutional as they are in breach of the fundamental right to privacy of correspondence and telecommunication[3]. Nevertheless, the court's decision does not affect the Directive itself. Data retention to the extent demanded by the Directive is not unconstitutional in the first place. To be exact, the court only ruled that the specific German legislation implementing the Directive did not meet the requirements of the German Constitution. It also did not judge the provisions under the ECHR. According to this judgment, transposition of the Directive is still possible (in Germany) as long as retained data is strictly limited to crimes that mean a threat to life or freedom of individuals or a threat to the country or one of its federal states. Also, the data has to be stored decentrally, using the highest security level possible at any given time. Judging from the tenor of the decision, it might be a good idea to implement exemptions for special groups like priests, doctors, lawyers, and even journalists as their business is affected mostly by the provisions in the Directive.

The Romanian Constitutional Court came to a similar conclusion with regards to the respective Romanian provisions on data retention, also taking Article 8 ECHR into account, which guarantees the right to a private life[4]. The court argued that the right to a private life necessarily implies the secrecy of the correspondence. Because those kinds of rights are only granted conditionally it is not the law itself which harms the right to a private life or to freedom of expression. Whoever uses his communication rights to e.g. commit a crime, cannot – of

▷ Prof. Dr. Thomas Hoeren, Münster. This text was written in September 2010 when the author was working as a visiting professor at the University of Akureyri (Iceland). The author would like to thank his colleagues in the media faculty, Markus Meckl and Birgir Gudmundsson, for assistance. Special thanks is also owed to Smari McCarthy from IMMI. Further information about the author at p. 160.

1 As stated on the IMMI website, s.a.

2 Directive 2006/24/EC, Article 6 – *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF.*

3 Federal Constitutional Court of Germany, 1 BvR 256/08 – "Vorratsdatenspeicherung", *www.bverfg.de/entscheidungen/rs20100302_1bvr02 5608.html.*

4 The Romanian Constitutional Court, Official Monitor no. 798, 23-11-2009 – CRi 2010, p. 49–51 with summary of and comments on the full decision available at *www.ccr.ro/decisions/pdf/ro/2009/D1258_09. pdf;* see *www.legi-internet.ro/english/jurisprudenta-it-romania/decizii-it/romanian-constitutional-court-decision-regarding-data-retention. html* for an unofficial english translation – last visited 10-08-2010.

course – possibly claim those rights to justify their unlawful actions. But the fact that data retention provisions treat all subjects of law equally makes data retention itself "likely to overturn the presumption of innocence and to transform *a priori* all users of electronic communication networks into people suspected of committing terrorism crimes or other serious crimes"[5]. That again would of course be against fundamental democratic principles.

It is not far to seek that under these premises Icelandic data retention laws might as well not withstand review under the ECHR. Effective changes need to be made here. The right approach is yet in question. One might either tend to go to the extreme and completely dismiss data retention from the agenda, or narrow it down to strictly limited purposes – the former in a way being the Swedish approach, the latter being the German approach. Although total rejection of data retention might be the most liberal solution, this would certainly impinge upon EU law. The European Commission has already filed a complaint against Sweden for inaction on the implementation of the Directive as Sweden did not implement the Directive within the given timeframe[6].

II. Liability

In terms of data retention and communication protection in general, one also has to answer the question of liability for wrongdoings. Iceland already has regulations on that in law 30/2002 on e-commerce and electronic services[7]. Under this law, hosting providers and telecommunication networks etc. are seen as "mere conduits" and thus enjoy the privilege of indemnity. This means, that they are generally not liable for whatever data is shifted through their services. Although there are only few and mostly well defined exceptions to this, the exception for general court orders without further definition is worrying.

1. EU E-Commerce Directive

Taking into account EU law, one has to consider Directive 2000/31/EC, better known as E-Commerce Directive[8]. Adopted in 2000, the Directive sets up an internal market framework for electronic commerce, providing legal certainty for business and consumers alike[9]. The relevant rules concerning liability of service providers etc. are found in Article 12 of 2000/31/EC. Given that the provided service only consists of transmission or provision of access to a communication network, a provider shall principally not be liable for the information transmitted even if the information infringes the law. Article 12 provides a few exceptions to this principle of no liability for mere conduits: As long as the provider does not initiate the transmission, select the receiver, or select or modify the information contained in the transmission, the respective service enjoys indemnity. For host providers, when the service consists of the storage of information provided by a recipient of the service[10], there is a simple knowledge test: As long as providers do not know of illegal content, they are neither liable nor obliged to perform an active search for illegal content.

2. US Notice and Take Down Approach

In the U.S. the so called "notice and take down" approach, which is regulated in sec. 512 of the Digital Millennium Copyright Act of 1998, is more common. This means that providers are not liable as long as they react on a notice or complaint, explicitly stating the relevant content, by deleting the content or index entry. U.S. law defines specific criteria for filing such a complaint[11]. A great disadvantage of this system is that it can be abused quite easily. On the one hand, sending out incorrect complaints to economically harm competitors seems to be common practice. Google has complained that more than half of the received takedown notices are business targeted and thus abusive[12]. On the other hand, false complaints may often be fulfilled without prior examination into the actual justification[13].

3. Exceptions to the EU-E-Commerce-Directive

The European Council recently recommended the implementation of notice and take down procedures for mere conduits as well[14]. However, this does not generally touch the principles set out in Articles 12-15 of the Directive concerning liability under mere conduit as notice and take down procedures shall only apply in cases of child pornography, racism and xenophobia or terrorist activities.

But there is another exception in the Directive: Article 12 (3) 3. of the Directive states that this principle does "not affect the possibility for a court or administrative authority, in accordance with Member States' legal systems, of requiring the service provider to terminate or prevent an infringement" with the law. It seems that even the EU Directive allows for general court orders without giving a definition under which exact circumstances such court orders are allowed.

Compared to the provisions in the Icelandic Act, it appears that Iceland has already adopted the EU Directive perfectly well. The Icelandic Act limits the liability for providers in respect of conduit almost word for word as does the Directive. Yet, what is not to be found is a provision that there are exceptions for general court orders. This can only be found in the Directive. Thus, there has to be a mistake in the proposal for an Icelandic Modern Media Initiative (furtheron IMMI proposal).[15] Especially with regards to the non-implementation of notice and take down, the current Icelandic Act is already very good. But problems might arise as soon as Iceland acquires full EU membership because the before-

5 *www.edri.org/edrigram/number7.23/romania-decision-data-retention* – last visited 10-08-2010.
6 *Olsson, Tobias/Olsson, Lova*, "Sverige stäms för datalagring" – SvD 26-05-2009 – *www.svd.se/nyheter/inrikes/sverige-stams-for-datalagring_2954845.svd*.
7 Cf. IMMI proposal.
8 *http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2000:178:0001:0016:EN:PDF*.
9 *http://ec.europa.eu/internal_market/e-commerce/directive_en.htm*.
10 Cf. Art. 14 1. Directive 2000/31/EC.
11 Cf. sec. 512 Digital Millennium Copyright Act of 1998 – *www.copyright.gov/legislation/dmca.pdf*.
12 Google submission hammers section 92A – PC World (New Zealand), 16-03-2009, *http://pcworld.co.nz/pcworld/pcw.nsf/feature/93FEDCEF6636CF90CC25757A0072B4B7*.
13 *Nas, Sjoera*, "The Multatuli Project ISP Notice & take down", 27-10-2004, *www.bof.nl/docs/researchpaperSANE.pdf*.
14 Draft Recommendations for Public Private Cooperation to Counter The Dissemination of Illegal Content Within the European Union, *www.edri.org/files/Draft_Recommendations.pdf* – last visited 10-08-2010.
15 The proposal is published on *www.immi.is*.

mentioned problems concerning court orders and monitoring duties to prevent future cases might influence Icelandic legal practice, although this is a topic which is generally much hated in the EU itself. Nonetheless current Icelandic law there are explicit rules missing on the liability for links and for forum and search engine operators, which should be implemented.

III. Process Protection – Libel Tourism

Concerning process protection and libel tourism the criticism in the IMMI proposal remains unclear. The point in question is why courts in the UK claim jurisdiction over publications or remarks that have been published or made in Iceland. But it is not pointed out how a new Icelandic law could possibly hinder courts in the UK to do so.

1. UK Defamation Law

Apart from this unclear criticism, the situation concerning UK defamation law is indeed problematic when it comes to defending against libel torts because it is deemed heavily in favor of the plaintiff[16]. Participation in legal battles is oftentimes very cost-intensive so that a publisher of alleged libelous material might refrain from defending themselves. This does not only apply in cases where the publisher is not economically capable to do so but also when it is simply not in their economic interest. On top of that, the outcome of a case cannot always be foreseen from the start. In the UK, this led to the introduction of conditional agreements between law firms and their clients referred to as "no win no fee" agreements. Those agreements put the duty to pay a lawyer's bill under the condition that the case is won. However, this does of course not affect the losing party's duty to pay for damages and expenses on the winning party's side. Unlike the defendant in a criminal case or other civil suits he is assumed to be in the wrong. Due to this presumption that derogatory statements are false, the defendant has to prove that the statements he made are true. The worrying effect: Plaintiffs under "no win no fee" practically gamble someone else's money under very limited risks[17]. On top of that, establishing defenses against libel allegations is often not so easy. The defense of "fair comment" is often hindered because comment is always subjective and not always easy to distinguish from facts which can naturally not be "fair" but are either true or false[18]. This sets defendants out to "the mercy of the caprice of juries and the malice of judges"[19].

2. European Approach

To understand the European perspective, one can first of all take a look at the case *Steel and Morris v. UK, also called the "McLibel case"* on 15 February 2005, before the ECHR. In the original case, McDonald's sued Steel and Morris for distribution of a pamphlet against McDonald's. Although McDonald's won before the English courts, Steel and Morris went before the ECHR, claiming violation of their right to a fair process as the process took ten years and resulted in excessive fees and damages. The ECHR found that this is a violation of Article 6.1 – the right to a fair hearing – and Article 10 – the right to freedom of expression – of the Convention. It stated that "it is essential, in order to safeguard the countervailing interests in free expression and open debate, that a measure of procedural fairness and equality of arms is provided for." The court found that an award of damages for defamation must be reasonably proportionate to the injury to the reputation suffered. Although the rewarded sum had never been enforced by McDonald's the fact that it remained enforceable led to the conclusion by the court that the award of damages is disproportionate.

3. Options for Iceland

The conclusions for the situation in Iceland are as follows. It is indeed possible for Iceland to refuse to recognize British judgments. Article 34 of the Lugano Convention, which Iceland signed, contains a provision about the so called *ordre public*, which sets the basic principles of domestic moral values or public policy. Pursuant the Lugano Convention a judgment issued in another member state shall be recognized in the other states. The only possible exception is when such a judgment is fundamentally contrary to public policy in the state in which recognition is sought. A concept of public policy is strictly national and ought to operate only in exceptional cases only for exceptional application so that the *ordre public* is only to be considered where the recognition of a judgment would infringe a fundamental principle. An example for a court ruling under the *ordre public* from Germany illustrates this. In 1992, the Federal Court of Justice of Germany – which can be referred to as the German Supreme Court – denied the enforceability of punitive damages under German law[20]. It argued that excessive damages would violate the constitution. A fundamental principle in Germany is that there is compensation for damages only for the restitution of the status quo ante. Nevertheless, there is no general rule on public policy. The application of the *ordre public* doctrine is always a matter of the specific case. That also means that it is not possible to enact a general law about that.

4. US Approach

In the U.S. the reverse principle is in force. There domestic courts in general shall not recognize a foreign judgment in defamation cases unless the domestic court determines that the defamation law applied in the foreign jurisdiction provided as much protection for freedom of speech and press in the relevant case as would be provided by the U.S. Constitution[21].

To sum these findings up: Iceland can refuse to recognize British court decisions under Article 34 of the Lugano Convention. As far as excessive fees in the UK are concerned, they violate the European Convention on Human Rights and besides those fundamental principles of Icelandic tort law. But there is one danger: As soon as Iceland acquires full EU membership the EU Directive 805/2004/EC will come into effect. In Article 6 this Directive creates a European Enforcement Order for

16 *Wheatcroft, Geoffrey*, "The worst case scenario", The Guardian, 28-02-2008 – *www.guardian.co.uk/commentisfree/2008/feb/28/pressandpublishing.law.*
17 Cf. ibid.
18 *Cf. Hunt v. Star Newspaper* [1908] 2 KB 309, Tab 3, at 319-320, CA.
19 *Wheatcroft*, loc. cit.
20 BGH, Judgment of 4-06-1992 – IX ZR 149/91.
21 Bill Text 111th Congress (2009-2010), S. 3518.IS, sec. 4102.

uncontested claims. This means that in those cases no member state can invoke *ordre public* any more.

A quite dubious topic in this context is called SLAPP which is an acronym for "strategic lawsuit against public participation". Those lawsuits aim at the intimidation and silencing of critics by burdening them with the costs of lawsuits[22]. The *McLibel* case is a typical example of such strategic procedural tactics. Typically in a SLAPP lawsuit the plaintiff does not even expect to win the case. In combination with a "no win no fee" agreement the defendant bears most of the costs for his defense against false allegations. Others might also be intimidated to participate in the debate, fearing that otherwise they might be sued as well. As those kinds of lawsuits pose a threat on the 1st Amendment right to free expression in the U.S. there are unique variants of anti SLAPP legislations in America[23]. Their aim is to protect legitimate litigants from procedurally coercive tactics. Problems arise, when the effect of anti SLAPP legislation reverses itself. Any defamation lawsuit might be considered as SLAPP so that the presumptive application of anti SLAPP laws is practically used as a defense. This can burden parties with meritorious claims and chill parties with nonfrivolous ones[24]. In *Palazzo v. Ives*[25] the court therefore stated: "By the nature of their subject matter, anti SLAPP statutes require meticulous drafting (...). There is a genuine double-edged challenge to those who legislate in this area." As the *McLibel* case has shown SLAPP as such is – of course – to be condemned in Europe as well. It is thus very questionable whether or not specific legislation is really necessary and whether it will be effective to prevent future SLAPPs.

IV. Publication Rule

The IMMI proposal states that the ECHR had confirmed that, for the purposes of the law of libel, an internet publication should be considered to be "published" afresh every time a reader views it. The ruling also found that libel proceedings brought against a publisher after a significant lapse of time may well, in the absence of exceptional circumstances, give rise to a disproportionate interference with press freedom.

The case the IMMI proposal refers to is *Times newspaper Ltd. (Nos 1 and 2) v. The United Kingdom*[26] before the ECHR. This decision refers to an old UK case from 1849 called *Brunswick v. Harmer*[27] which laid down the common law rule that each publication of a defamation gives rise to a separate cause of action. In 2001 the British High Court indeed held that internet material is published anew every time it is accessed[28], known by now as the "internet publication rule". The counter concept to this rule is the "single publication rule". Despite of that, the case remains a mere national UK case which is on top of that based on a very old precedent. The ECHR does not really confirm the internet publication rule – as is stated in the IMMI proposal – it only says that the interpretation of "publication" by the UK courts does not violate the Convention.

The IMMI proposes to restrict the possibility to file a lawsuit on two months after publication. But this does not solve the problem at all because the definition of publication still remains unclear. Besides, it is to be born in mind that Iceland can refuse to recognize British decisions like *Times* under Article 34 of the Lugano Convention anyway. So if a change of law should really be deemed necessary, one should rather link the restriction to knowledge than to publication: A change of the Civil Procedure Act could provide for a clause that injunctions can only be granted within a short period of time after the plaintiff knows or should know the content on the web.

V. Whistleblowers' Protection

Whistleblowing means raising concerns about wrongdoing occurring in an organization or body of people. As an example, wikileaks.org has recently come to mainstream fame, publishing worrying internal documents of the U.S. Forces about the Iraq War whilst keeping the sources anonymous. Whistleblowing can be either internal or external: internal meaning reporting wrongdoing to officials etc. inside the organization itself, external meaning making the information available to the public. The goal of whistleblowing schemes is to protect whistleblowers from retaliation by their superiors or employers. As stated in the IMMI proposal, Iceland plans to change "laws regarding the rights and duties of official employees (no. 70/1996) such that official employees be allowed to break their duty of silence in the case of extreme circumstances of public interest. Similar changes could be made to municipal governance law (no. 45/1996) regarding employees of municipal governments."[29]

The EU Article 29 Group – or Article 29 Data Protection Working Party, short WP 29 – has issued an opinion on 1 February 2006[30], dealing with the issue of compliance of internal whistleblowing schemes (such as whistleblowing hotlines or websites) with EU data protection rules set out in Directive 95/46/EC[31]. That applies to whistleblowing schemes in the fields of accounting, internal accounting controls, auditing matters, fight against bribery, as well as banking and financial crime.

Under Article 7 of the Directive, companies must take all reasonable technical and organizational precautions to secure, that data processing is secure and kept confidential. Article 7 (f) of the Directive requires balancing the legitimate interests pursued by the processing of personal data on the one hand and the fundamental rights of the data subject on the other. This balance of interest test should take various issues into account, such as proportionality, subsidiarity, the seriousness of the alleged

22 *www.onthemedia.org/transcripts/2010/04/02/07* – last visited 11-08-2010.

23 Cf. e.g. sec. 425.16 of the California Code of Civil Procedure – *www.casp.net/statutes/cal425.html*; for further reference to anti SLAPP laws in other states see *www.legal-project.org/149/anti-slapp-statutes-in-the-us-by-state*.

24 *Navellier et al. v. Sletten*, 29 Cal.4th 82, 124 Cal.Rptr.2d 530, 52 P.3d 703, 29-08-2010 – dissenting opinion – *www.casp.net/cases/Navellier%20v.%20Sletten%201.html*.

25 944 A.2d 144 (R.I. 2008).

26 *www.pacelegal.com.au/tag/times-newspapers-ltd-nos-1-and-2-v-united-kingdom-applications-300203-and-2367603*.

27 *Duke of Brunswick v. Harmer* [1849] 14 QB 154.

28 *Godfrey v. Demon Internet Limited*, CRi 2000, p. 56 with remarks by *Lloyd* = [2001] QB 201.

29 Cf. IMMI proposal.

30 *http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2006/wp117_en.pdf*.

31 *http://ec.europa.eu/justice_home/fsj/privacy/docs/95-46-ce/dir1995-46_part2_en.pdf*.

offenses that can be notified and the consequences for the data subjects. What will also be necessary are adequate safeguards, as Article 14 of the Directive provides that when data processing is based on Article 7 (f), individuals have the right to object the processing of data relating to them at any time if there are compelling legitimate reasons[32]. Acknowledging that whistleblowing schemes may be a helpful tool for organizations to monitor their compliance with various regulations the WP 29 emphasizes, that all whistleblowing schemes must comply with EU data protection law. In the implementation of whistleblowing schemes the fundamental right to the protection of data, in respect to both the whistleblower and the accused person, must thus be ensured throughout the whole process of whistleblowing[33].

That means that although EU law does not provide for an obligation to implement general whistleblowing schemes, Iceland must comply with the provisions laid down by the EU data protection directive, should it choose to realize such a system. It has to take into account the need for protection of the person concerned, fair procedure, and the right to object data processing on reasonable, legitimate grounds. From this it follows that a very difficult balancing of interests will be necessary. The U.S. model can again serve as a bad counterexample: As data protection concerns are much less pronounced, U.S. whistleblowing schemes might often be not in full compliance to EU data protection provisions.[34]

VI. Further Topics

Further topics which are raised in the IMMI proposal but which are not dealt with here are a new Freedom of Information Act and regulations on cloud computing. Misleading remarks in the proposal have been made regarding the protection of journalistic sources in Iceland. Here the authors of the proposal stated that Icelandic jounalists have to name their sources on the basis of any court order. However, the Act on Criminal procedure 109/2008 provides that the court can only demand a disclosure on the basis of higher vital interests of the state. Finally, a new modern media-law might require special training of judges which is a problem in Iceland. And at the end the question remains whether the current technical infrastructure is capable to make Iceland a safe harbor for the protection of freedom of expression and information at all. To have free offices in Kevlavik and good weather conditions for building up server farms might not be enough for building up a "Switzerland of bits". But nevertheless: The Icelandic vision is of high importance for Europe – in order to check the opportunities for internet governance and a liberal media regulation within the EU.

32 Cf. p. 9 of the opinion, loc. cit.
33 Cf. p. 18 of the opinion, loc. cit.
34 Cf. *Marchini, Renzo*, "Conflict of Laws: Anonymous Whistleblowing Hotlines under Sarbanes Oxley and European Data Protection Laws", Privacy & Data Security Review, May 2006, p. 309-313.

Case Law

USA: Distinction between Software Sale and Software License

17 U.S.C. §§ 106, 109, 117

Editor's Headnote

A software user is a licensee rather than an owner of a copy where the copyright owner

(1) specifies that the user is granted a license;

(2) significantly restricts the user's ability to transfer the software; and

(3) imposes notable use restrictions.

Court of Appeals for the 9th Circuit, decision of 10 September 2010 by *Canby, Callahan* and *Ikuta*, Circuit Judges

Timothy Vernor v. Autodesk, Inc. [No. 09-35969; D.C.No. 2:07-cv-01189-RAJ]

Facts

Timothy Vernor purchased several used copies of Autodesk, Inc.'s AutoCAD Release 14 software ("Release 14") from one of Autodesk's direct customers, and he resold the Release 14 copies on eBay. Vernor brought this declaratory judgment action against Autodesk to establish that these resales did not infringe Autodesk's copyright. (...)

I.A. Autodesk's Release 14 software and licensing practices

The material facts are not in dispute. Autodesk makes computer-aided design software used by architects, engineers, and manufacturers. It has more than nine million customers. It first released its AutoCAD software in 1982. It holds registered copyrights in all versions of the software including the discontinued Release 14 version, which is at issue in this case. It provided Release 14 to customers on CD-ROMs.

Since at least 1986, Autodesk has offered AutoCAD to customers pursuant to an accompanying software license agreement ("SLA"), which customers must accept before installing the software. A customer who does not accept the SLA can return the software for a full refund. Autodesk offers SLAs with different terms for commercial, educational institution, and student users. The commercial license, which is the most expensive, imposes the fewest restrictions on users and allows them software upgrades at discounted prices.

The SLA for Release 14 first recites that Autodesk retains title to all copies. Second, it states that the customer has a nonexclusive and nontransferable license to use Release 14. Third, it imposes transfer restrictions, prohibiting customers from renting, leasing, or transferring the software without Autodesk's prior consent and from electronically or physically transferring the software out of the Western Hemisphere. Fourth, it imposes significant use restrictions: