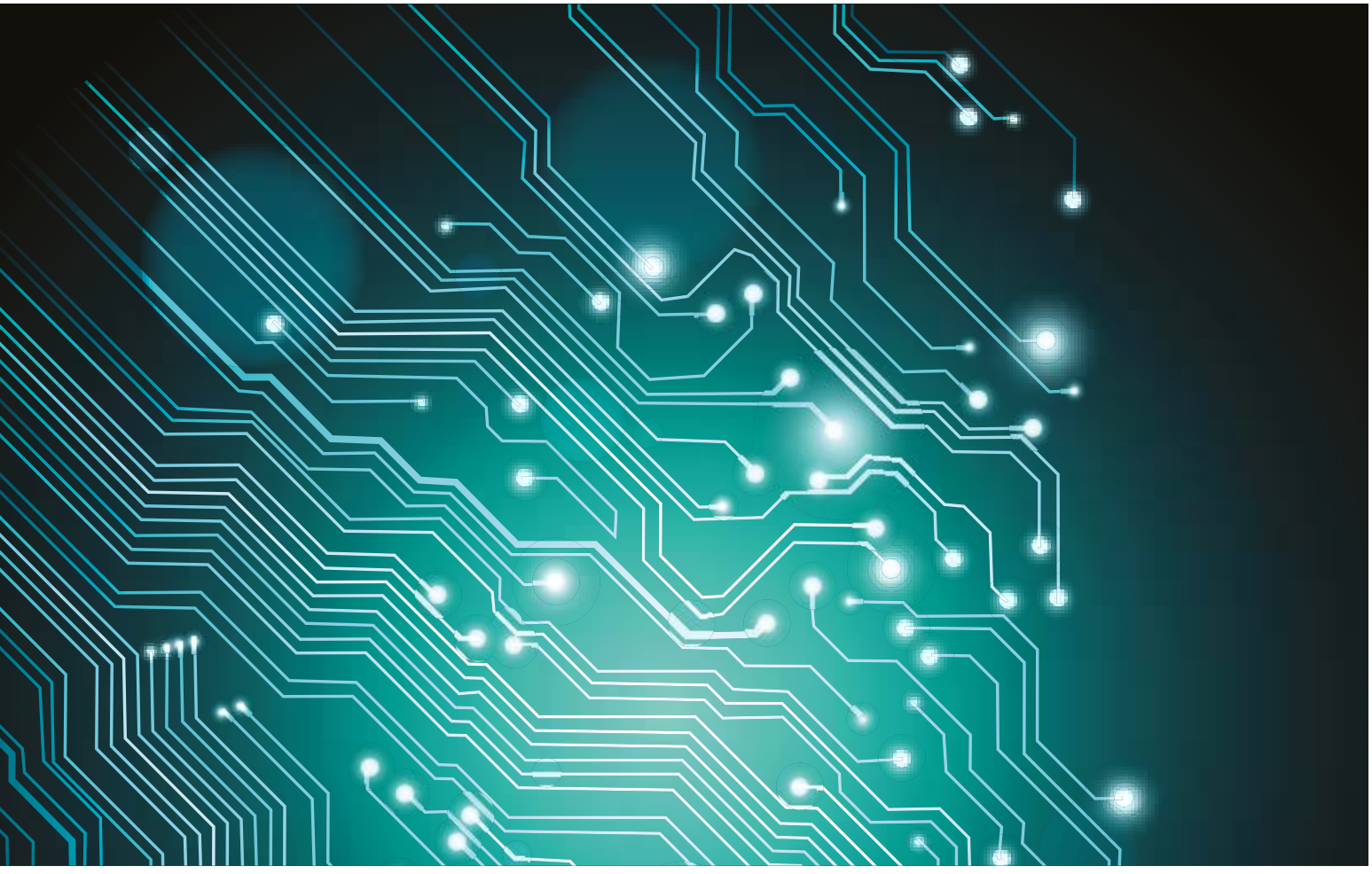
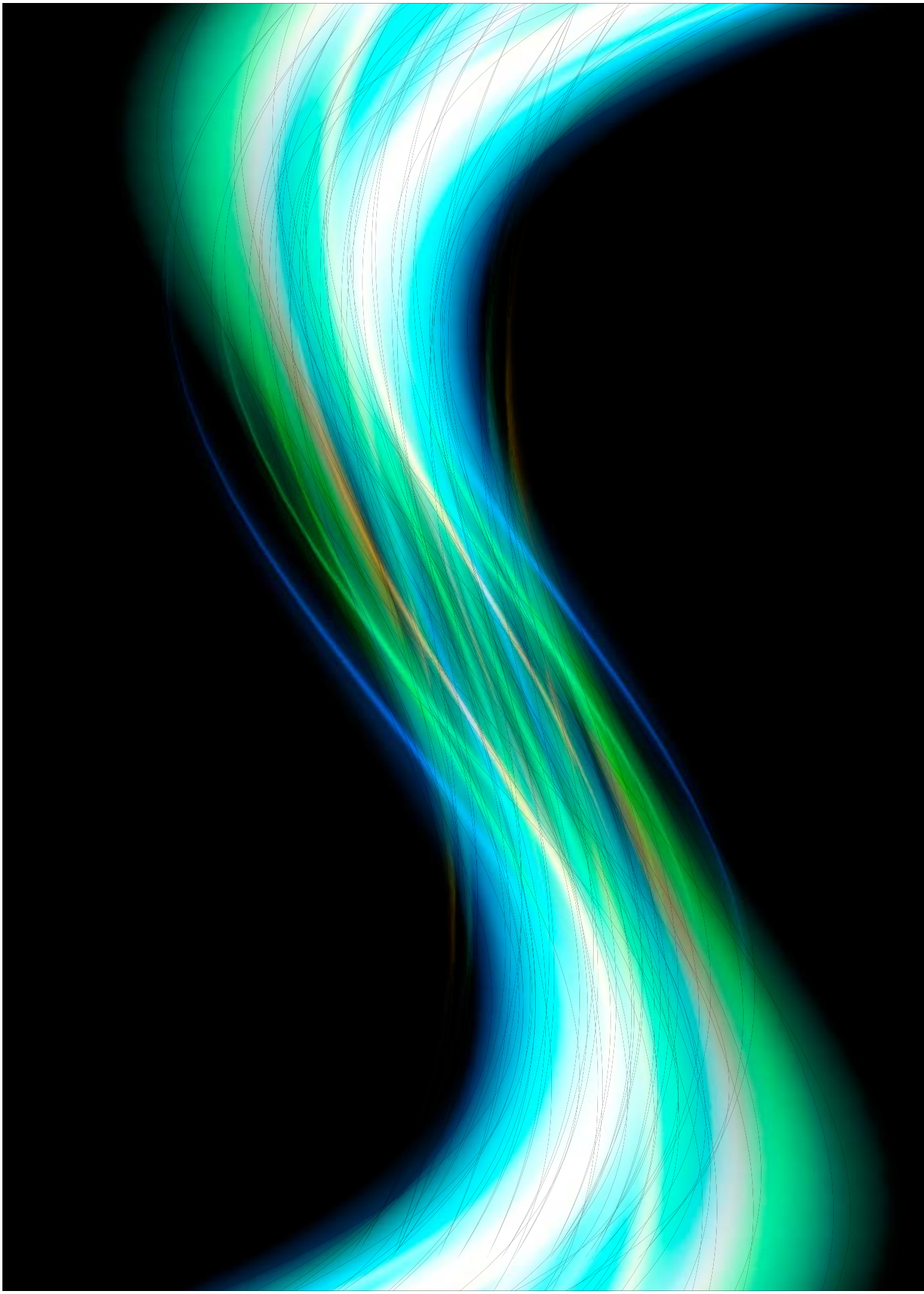
SETTERWALLS

IP Tech

REPORT

Summer | 2015





Introduction

We are pleased to present another issue of the IP Tech Report, in which members of the Setterwalls' IP Tech group comment on selected legal topics in relation to technology and intellectual property.

In this issue of the IP Tech Report you can read about driverless cars which raises ceratin data privacy concerns. You can also learn about legal considerations to take into account when launching a new app. The report also contains an update of the development of the unitary patent protection in the EU. These are just some of the interesting articles in the field of IP Tech area.

Setterwalls' IP Tech group continuously and closely monitors all the issues raised in our reports as well as many other questions in the IP Tech area. You are always welcome to contact us to discuss how your business can best meet its legal challenges.

Fredrik Roos, partner and head of Setterwalls' IP Tech practice group together with Jörgen Axelsson, partner, and Lennart Arvidson, partner.
fredrik.roos@setterwalls.se
jorgen.axelsson@setterwalls.se
lennart.arvidson@setterwalls.se

Are you launching an app? Policies and pitfalls

In addition to the technological considerations, there are also several legal considerations to be taken into account when launching a new app. As is elaborated below with regard to the two main platforms, App Store and Google Play, it is essential for the publisher to include the outcome of such legal considerations in a customised end-user licence agreement (EULA).

The Platforms

On App Store, a standard EULA is provided, and applies to apps that are made available on the platform. This agreement covers some of the main aspects of licensing, but the content makes it clear that the main objectives are to minimise Apple's obligations and to indemnify the company from claims relating to the use of apps. As two examples of parts that are not in the best interests of the publisher, the standard EULA leaves out the matter of processing personal data and refers to definitions in American copyright legislation even in the Swedish version of the agreement.

It is safe to say that there are gains to be made from creating an EULA on the basis of the characteristics of the app and the specific needs of the publisher. The standard EULA allows for such an alternative by stating that it applies unless there is a valid, customised EULA between the consumer and the publisher, in which case the standard EULA will not apply at all.

Two important points must be made with regard to this provision. First, the customised EULA must meet certain requirements set out by Apple in order to be deemed to be valid. Secondly, as the standard EULA will not apply at all when a customised EULA satisfies the minimum requirements stated by Apple, the provisions in the latter agreement must cover all aspects of licensing, including those that were regulated satisfactorily in the standard EULA. With Google Play, the situation is different. There is no standard EULA provided for apps on this platform, and Google therefore strongly advises publishers to submit their own. Similarly, as with Apple's minimum requirements, every publisher on Google Play has agreed to the Google Play Developer Program Policies. When creating a customised EULA, the publisher must establish that the agreement is fully compliant with these policies as well as with all applicable laws and regulations.

Key Provisions

There are a number of legal issues to bear in mind when creating a customised EULA. One crucial question is to decide to what extent the rights of the copyright owner are to be licensed to the end-user. In this regard, freedom of choice is considerably limited by Apple's minimum requirements, and the corresponding provision in the standard EULA might therefore serve as a model to ensure that the provision that is drawn up does not cause the entire EULA to become invalid on App Store.

Another important aspect is the processing of personal data. The publisher needs to consider what personal data will be collected and processed within the app, and ensure that this processing complies with the applicable legislation. As stated in the Swedish Personal Data Act (1998:204) (Sw. Personuppgiftslagen), the processing of personal data generally requires consent from the person that the information relates to, and there is some personal data that is not allowed to be processed at all. For a publisher with a website, the EULA may very well make a reference to the privacy policy of that website by including a clickable link, after making the modifications to the policy deemed necessary owing to the scope of the app.

Apart from other essential points, such as limitation of liability and regulation of governing law, there is one relatively new aspect which it is necessary for publishers within the EU to observe. Since the Consumer Directive (2011/83/EU) came into force during last year, consumers have a right to withdrawal within 14 days of purchasing any digital content from a company within the union. In other words, consumers are able to pay for and download an app, use it for 14 days and then get a full refund when they return it. Luckily, the Consumer Directive provides for an exception if consumers, prior to using the app, expressly consent to losing their right of withdrawal upon first use.

In conclusion, submitting a customised EULA may provide great advantages for a publisher on App Store, and is vital for a publisher on Google Play. At the same time, the liberty in the process of creating such a document is significantly restricted by law and contractual provisions between the publisher and the companies responsible for the platforms. Every publisher should therefore ensure that their customised EULA is regarded as valid and compliant with the applicable legislation, while safeguarding all of the publisher's interests.

Carl-Johan Bune and Marcus Svensson,
members of Setterwalls' IP Tech Practice Group.
carl-johan.bune@setterwalls.se
marcus.svensson@setterwalls.se

Unitary patent protection

A single patent title, to make the EU more competitive as regards the US and Japan, has long been under discussion. The 17th draft of the rules of procedure has recently been published and this version is deemed to have the support of all the participating states as the preparatory committee has made the changes to this draft that they considered necessary.

The EU has been discussing a single patent title providing uniform protection throughout the EU for at least 30 years. It seems as though we have now reached a conclusion in the signing of the Unified Patent Court ("UPC") Agreement. The UPC Agreement was approved within the EU in December 2012 together with a regulation creating unitary patent protection (Regulation 1257/2012) and a regulation establishing language rules. These three instruments have been referred to as the EU patent package. Sweden ratified the UPC Agreement on the 5th of June 2014.

Unitary patents will be granted by the European Patent Office (EPO) but will constitute a single patent title providing uniform protection and equal effect. The patentability requirements and terms of protection will be the same as for the European patents of today. To obtain a unitary patent, entry in the Register for Unitary Patent Protection must be requested from the EPO within one month of the patent being granted.

The creation of the UPC is the basis for enforcement of unitary patents. However, the UPC will also have jurisdiction over the enforcement of existing European patents. The court system will include a Court of First Instance and a Court of Appeal. What are known as Local and Regional Divisions form a part of the Court of First Instance. In addition there is a Central Division in Paris with departments in London (for, inter alia, pharma-related issues) and Munich (for mechanical engineering). At the time of ratification each contracting state must clarify whether they are setting up a Local or Regional Division. In March 2014 Sweden, Estonia, Latvia and Lithuania signed an agreement on the establishment of a Nordic-Baltic Regional Division of the UPC, which would be located in Stockholm. The language of the proceedings will be English. The Court of Appeal for the UPC system will be based in Luxembourg.

Decisions under the UPC system will be effective and binding in all participating states. This means that a revocation of a patent or a decision concerning infringement will have effect in all participating member states. The UPC will handle cases concerning both unitary patents and European patents, including previously granted patents, following a transition period of seven years from the date of entry into force of the UPC Agreement. During the transition period, holders of traditional European patents may opt out of the UPC system. An opt out means that a European patent will remain subject to the national system we know today. However, a patent-holder may at any time during the aforementioned transition period choose to opt into the UPC system.

Spain has lodged two appeals against the regulation, however, on the 5th of May 2015, the Court of Justice dismissed Spain's actions which means that the implementation process is further on its way.

However, there is still a way to go before the system becomes operational. Before the unitary patent comes into effect 13 states, including France, Germany, and the United Kingdom, are required to ratify. France is the only country of the required states that have ratified so far. Furthermore, on May 8th 2015 the preparatory committee launched a written consultation process on the fee structure of the court. The users now have 12 weeks to give their feedback on the consultation. IP/Tech Report will cover the development.

Lennart Arvidson and Lovisa Nelson,
members of Setterwalls' IP Tech Practice Group.
lennart.arvidsson@setterwalls.se
lovisa.nelson@setterwalls.se

Swedish Dairy vs. Oatly – who is crying over spilled milk?

There has been a row going on in the Swedish Market Court. The Swedish Dairy Association, referred to below as "Swedish Dairy", is suing Oatly for violations of the Swedish Marketing Practices Act. Oatly manufactures products based on oats, which can be used as substitutes for dairy products – such as milk, cream, yogurt, crème fraiche, etc. Swedish Dairy's "beef", pardon the pun, concerns claims about milk, which Swedish Dairy claims are misleading and offensive to the dairy business. The following are examples of the claims in question:

"It is like milk, but made for humans."

"No soy. No milk. No harm."

"No cream, soy, rice, almonds or any other ephemeral inventions."

"… our fraiche provides an upgrade to crème fraiche and, if you wonder what we mean by upgrade, we mean that you get the same great performance, but our fraiche is lighter, cleaner and healthier."

This article is not about who is right and who is wrong. That would be tantamount to second-guessing the decision of the Market Court. What we would like to comment on are two lessons learned in this case.

Lesson 1: Preliminary injunctions – not if you mess with the security placed

Swedish Dairy has asked for a preliminary injunction against the first two claims above. Twice. Both times, the Market Court has denied the motion.

The first time around, the security was in the form of a bank guarantee of SEK 1 million. The way it was worded, it related to the damage Oatly would be able to prove it had suffered as a consequence of the preliminary injunction if Swedish Dairy prevailed. The guarantee designated the writ of summons in the Market Court and the preliminary injunction. So far so good. However, it was also stated that, in order to be valid, the claim for compensation had to be made to the bank in question, Swedbank AB, no later than 90 days after the "judgment or decision of the case" had become final.

The Market Court interpreted the wording of the guarantee to mean that the time limit of 90 days should be counted from the day of the Market Court's final decision in the matter. The Market Court pointed out that it is unlikely that a decision concerning damages can be obtained within that time frame. Had it been 90 days counting from when a decision awarding damages to Oatly had become final, the time frame would have been acceptable. The Court also found that the amount of SEK 1 million was insufficient to cover the potential damages.

Swedish Dairy is not a quitter, however. So it got back up on its horse … sorry, cow, and filed for a preliminary injunction a second time.

This time, the bank guarantee was in the amount of SEK 5 million – which the Court found to be sufficient as such. The 90 days were to be counted from the day Swedish Dairy's liability (following the interim injunction) had been finally determined by means of a Court decision or settlement between the parties. So far so good. However, this

> *Get off your horse and drink your milk*
>
> *John Wayne*

time there was an added limitation to the guarantee's validity. It was only valid for three years after the Market Court had rendered its judgment.

The Market Court referred to case law from the Swedish Supreme Court, in which it was held that a corresponding limitation of five years had not been accepted. Also, the Market Court noted that the guarantee was only valid if the case was settled by means of a judgment, not taking into account that the Market Court may settle the case by means of a decision.

Thus, two strikes. It remains to be seen whether Swedish Dairy will try for a third time to get a different result. However, it goes to show that limitations as to a guarantee's validity in time or amount may cause a court to deny a preliminary injunction. If you are seeking a preliminary injunction, do not serve skimmed milk as compensation, serve whole milk with cream on top or, to put it another way and in the context of a bank guarantee, the validity should be no less than 90 days after liability to pay damages has been determined, and, if you seek to limit the validity generally in time, the rule of thumb should be more than five years (one should probably opt for ten as the general amount of time to be prescribed in Sweden) from the Court's final judgment or decision in the case. Bear in mind that a bank guarantee can always be recalled/released should the corresponding claim have been settled or the obligation against which it stands be nullified.

Lesson 2: Consider the general public's and media's view of your actions

The other rather more amusing thing about this case is how Oatly has chosen to be completely open with information in this case. It has published all writs and decisions to date. (they are available at http://oatly.com/daligstamningi-kyldisken/ (in Swedish)) and also made the case public by advertising in three major Swedish newspapers. That seems to have worked well for them, too. So far, speculation has been that Oatly may well have the last laugh.

Soon after Swedish Dairy filed its writ of summons, there was a new scientific study published concerning milk. The results probably gave a number of fervent supporters of milk pause for thought, as it indicated that milk is perhaps not as good for you as you might have thought. Most likely, however, this study will be refuted by another study, which in turn will be refuted by another study, and so on. That is just the way things seem to go. Still, Swedish Dairy's lawsuit comes at a time when milk, which as a product has been held dear by Swedish consumers for years and years, like a lot of other food produce is being questioned on nutritional, health and environmental grounds. Also, you have to admit that even though milk can be enjoyed by humans and may have nutritional benefits for us, it was not really made for us originally, was it? As Orwell put it, "Man is the only creature that consumes without producing. He does not give milk, he does not lay eggs, he is too weak to pull the plough, he cannot run fast enough to catch rabbits. Yet he is lord of all the animals." (George Orwell – Animal Farm)

So, judging from the media reaction (including social media), it could be that Oatly will be the real winner even if it should lose in court. Thus, a pyrrhic victory, if ever there was one – or will be one – for Swedish Dairy. This case proves that the way a case may play out in the media is worth considering as part of your litigation strategy. Not only do you have to know and use the law, you have to manage or even predict the media angle as well.

What is certain in this case is that the publicity so far has resulted in a rise in sales of Oatly products and that Oatly has received positive attention in the media – attention which, as the saying goes, no realistic advertising budget could buy. At Oatly, no one is crying over spilled milk.

Per Lidman, member of
Setterwalls' Life Sciences Group
per.lidman@setterwalls.se

The cloudy future of government IT

In recent years there has been an ongoing debate in Sweden regarding personal data and the implications for cloud computing and cloud-based services. However, it is not only personal data that becomes problematic when moving information to the cloud – a recent decision from the Swedish Parliamentary Ombudsman (Sw.: Justitieombudsmannen) ("JO") raises many questions when it comes to the possibility of Swedish public authorities, government agencies and municipalities (collectively "public sector bodies") purchasing IT and using cloud-based services. Cloud suppliers aiming to sell cloud-based services to customers in Sweden should be aware of this debate.

For public sector bodies in Sweden, information that is being processed in the cloud is subject not only to the Personal Data Act (Sw.: Personuppgiftslagen), but also to the Public Access to Information and Secrecy Act (Sw.: Offentlighets- och sekretesslagen) regulations. According to this particular Act, public sector bodies have an obligation to disclose public records to anyone who requests access to such records. When public sector bodies receive a request for disclosure, they have to make a mandatory secrecy assessment to ensure that the request for disclosure should not – depending on the circumstances of the specific case – be rejected due to secrecy obligations in accordance with the Act in question.

An issue that has been up for discussion is whether it is a requirement that the Swedish public sector bodies should perform a mandatory secrecy assessment prior to information being disclosed to a cloud supplier, or whether a cloud supplier should be considered as connected with the public sector body as such, and therefore automatically bound by the regulations concerning public access and secrecy. The answer to this question will be crucial in evaluating whether Swedish public sector bodies' use of cloud-based services complies with Swedish legislation.

New decision from the Swedish Parliamentary Ombudsman

JO concluded in a recent decision that some public health care providers were not legally entitled to commission a cloud supplier to work with medical record entries. The public health care providers had commissioned the cloud supplier to transfer recorded notes dictated by doctors to patients' medical records in order to shorten the time it took for a recorded note to be registered in the medical records. The process was handled electronically and no information was stored outside of the health care providers' IT-systems.

Both the cloud supplier and its employees were bound by a secrecy agreement, and had data processing agreements in place with the public health care providers. Given all the facts of the situation, JO concluded that the actions undertaken by the public health care providers constituted a disclosure of information to the cloud supplier and its employees.

JO further stated that the secrecy agreements in place were inadequate in this case. This was owing to the lack of sanctions to which the cloud supplier and its employees were subject. In contrast with the public health care providers' employees, the cloud supplier's employees were not subject to sanctions according to the Public Access to Information and Secrecy Act and the Swedish Penal Code (Sw.: Brottsbalken).

Impact assessment

This recent decision has sparked controversy regarding the impact the JO decision might have. Some argue that the decision constitutes a general obstacle for Swedish public sector bodies that are subject to the Public Access to Information and Secrecy Act to commission private entities to process or access data. This would be an obstacle that would prevent most public sector bodies from moving towards cloud-based services.

Others consider the decision to be more of a one-off case. The JO case concerned "highly sensitive information" and one could argue that the secrecy agreement in this specific

case was not drafted tightly enough. It would thus not mean that other cases should be treated in the same way.

Also, one could argue that the JO case should not have an impact on cloud-based services since in most cloud-based services, a cloud supplier does not access information the way the cloud supplier did in that particular situation, which involved listening to recordings of dictated notes. Even if the cloud supplier's employees technically have the possibility of accessing the information that has been stored, there are usually both technical security measures and instructions and agreements in place limiting such access.

Conclusion

It is not clear how and to what extent the JO case in question might impact on cloud-based services in general. Nevertheless, Swedish public sector bodies need to consider both the Personal Data Act and the Public Access to Information and Secrecy Act when considering storing information in the cloud.

Furthermore, it is not clear how strictly the Public Access to Information and Secrecy Act should be interpreted and in what circumstances it could constitute an obstacle to public sector bodies using cloud-based services for storing information regulated by the Act.

It is important for cloud suppliers offering cloud-based services to Swedish public sector bodies to be aware of the ongoing debate regarding their ability to use cloud-based services. The outcome of this debate could have an impact on how a cloud supplier might choose to develop its services in order to meet the requirements of a Swedish public sector body, e.g. with regard to the level of protection given to any information stored, how unauthorised access to and usage of information can be prevented, how employees are instructed to handle the information and regulations regarding liability for data loss.

Agnes Andersson Hammarstrand, member of Setterwalls' IP Tech Practice group
agnes.a.hammarstrand@setterwalls.se

Driverless cars – an area for data privacy concern?

Shortly we could be watching the latest episode of Game of Thrones while the car safely and smoothly takes us home. The driverless car comes with a lot of obvious benefits, such as reduced congestion and making the roads safer, in that it removes the biggest cause of traffic accidents – human error. However, driverless cars will depend on integrated software and GPS information in order to function properly. A permanent Internet connection and the GPS will enable the car to be traced, which raises data privacy concerns. Hence, the technique that enables the car to be driverless may be what puts obstacles in its way.

What is the concern?

In order to function and deliver a safe ride, driverless cars need to process and collect a huge amount of data. The car knows that you stopped to fill up the tank this morning and that you are most likely to drop by the gym on your way home. This raises concerns regarding data ownership, why you will want to make sure that such data is not used without your consent. But, who owns the data? This is not certain since there are several parties involved, such as the car manufacturer, the owner of the platform on which the data is processed and the individual who owns the car. Furthermore, if driverless cars are not owned by the user but provided as a service, what happens to the ownership of data then?

It is not just data ownership that could be a concern. Driverless cars raise a number of questions relating to the protection of privacy and to data compliance. The fact that cars, more than many other devices, are likely to have several different users, raises questions such as the need for consent to the processing of data every time the car ignition is switched on. The concept of driverless cars also raises the issue of how to guarantee that proportionate and adequate protection of the individual's privacy is maintained in this world of constant technical evolution.

Another aspect to consider is that problems and bugs in the software that the vehicle relies on may be a matter of life and death. Postponing sending software updates to the vehicle until it passes an Internet connection could lead to avoidable accidents. With regard to this, the software owner may want to have a function enabling the push of software updates to the vehicle as soon as the updates are ready. A driverless car equipped with a permanent Internet connection may also be alerted to hazardous conditions such as slippery roads and be provided with live traffic updates that allow the vehicle to automatically recalculate the route to avoid traffic jams. For this to be possible a constant tracking of movements is required. Is this even allowed?

It has been argued that we as consumers already have adopted technology that allows the tracking of our movements: the mobile phone. Our mobile operators need to know where we are at all times in order to deliver incoming calls. Thus, the same development is predicted for driverless cars. Considering the amount of data involved, entry into the automotive industry by companies like Apple and Google starts to make sense.

From product to service – a trend also in the automotive industry?

It is well-known that the digital economy and the mindset it brings with it enable many industries to go from product to service. Pharmaceutical companies are no longer limited to 'offering pills' to people who are ill but can also focus on

'offering pills' in order to maintain health (thereby expanding their consumer base). Is this a trend also in the automotive industry? Well, the automotive industry has started a slight shift, or at least an expansion of its focus, from offering the vehicle as a product to using the vehicle as a platform from which it provides services. In other industries where a supplier used to supply a product embedded in a bigger context, the shift would be to offer the service in order to prevent the product from coming to a standstill or failing.

Products serving as a platform for providing services, such as driverless cars, also open up the possibility of allowing third parties to provide services on the platform. From this perspective, additional privacy concerns arise given the increased number of entities processing people's personal data.

Concluding remarks

Under current and future data protection regimes, users will need to be informed of how their personal data is to be used, the purposes of the use and the recipients of any resulting information. In some cases the user's explicit consent will be required. Considering the hefty fines proposed in the European Data Protection Regulation – expected to amount to 5% of global annual turnover – driverless cars will need to be developed with privacy by design and privacy by default in mind such as has never been seen before.

Bobi Mitrovic and Linda Dahlin, members of Setterwalls' IP Tech Practice group.
bobi.mitrovic@setterwalls.se
linda.dahlin@setterwalls.se

Facts and figures

Established in 1878, Setterwalls is the oldest law firm in Sweden. Today it is also one of the largest law firms in Sweden, employing more than 190 lawyers at offices in Stockholm, Göteborg and Malmö. Setterwalls has undergone substantial expansion over the past 10 years, both in terms of the number of lawyers and practice areas. Setterwalls' dynamic growth and the firm's participation in several high-profile cases and transactions have pushed the firm to its prominent position in the Swedish legal services market.

Setterwalls is organized into practice groups and trade and industry oriented teams.

Setterwalls provides legal services to all players in the IT and telecom sectors including telecom operators, Internet providers, e-commerce companies, and manufacturers of hardware as well as computer software development companies. Setterwalls also regularly assists our other clients in IT-related matters such as procurement of systems solutions, and IT services. The IP Tech group is top ranked (tier 1) in Legal 500, 2015. According to clients interviewed by Legal 500 our TMT (Technology, Media and Telecom) group has "possibly the best team in the Nordics". Chambers Europe meanwhile speaks of our lawyers as *"The team is great: really skilful and fast-working."*

The IP Tech group is one of the firm's priority groups and has had a great deal of success during the last 10 years with a number of high profile matters. The group currently consists of 14 partners and 26 associates.

Practise areas

Aviation
Commercial
Corporate
Dispute Resolution
Employment & Labour Law
Energy & Commodities
Environment
Equity Capital Markets
EU & Competition Law
Financial Markets
Infrastructure & Construction
Insolvency & Restructuring
Insurance & Reinsurance
Intellectual Property Rights & Marketing Law
Life Sciences
M&A
Private Client
Private Equity
Public Procurement
Public Sector
Railway
Real Estate
Real Estate M&A
Shipping
Sports & Entertainment
Tax
Technology, Media & Telecom
Transportation

Contact

Setterwalls Advokatbyrå AB

STOCKHOLM
Arsenalsgatan 6
P.O. Box 1050, SE-101 39 Stockholm
T: +46 8 598 890 00
F: +46 8 598 890 90
E: jorgen.axelsson@setterwalls.se

GÖTEBORG
Sankt Eriksgatan 5
P.O. Box 11235, SE-404 25 Göteborg
T: +46 31 701 17 00
F: +46 31 701 17 01
E: fredrik.roos@setterwalls.se

MALMÖ
Stortorget 23
P.O. Box 4501, SE-203 20 Malmö
T: +46 10 690 04 00
F: +46 10 690 04 70
E: lennart.arvidson@setterwalls.se

www.setterwalls.se