THE LEGAL TECHNOLOGIST

ISSUE NO. 5 JUNE 2019

FEATURES

ARTICLE

Desert Life

Nick Cronjaeger, Head of Software Solutions at Thomson Reuters, gives an insight into his work and life in Dubai.

INTERVIEW

Blocking Crime

Eaindra Cho interviews Chris Recker about cyber crime and blockchain in this month's featured interview.

Our Staff.

Editor
Marc May

Junior Editor
Rebecca Baker

Marketing Manager
Eaindra Cho

Contributors
Nick Cronjaeger
Motunrayo Akinyemi
Chris Recker
Caroline Calomme
Steven O'Donnell
Simon Pecovnik
Roderik Plukker
Birgit Verbeek
Catherine Firmin
Alice Namuli Blazevic

Front Cover

Wanderer above the sea of fog by Caspar David Friedrich

Website
http://www.legaltechnologist.co.uk
Twitter
http://www.twitter.com/LTechnologist
Facebook
'The Legal Technologist'
Email
marc@legaltechnologist.co.uk

Insight into the future of law

The Legal Technologist

A note from the editor

Legal technology is shaping and modernising legal professions around the world. This magazine aims to bring together a diverse mix of international opinion, and we are lucky to have articles from Uganda, Nigeria, Dubai, the Netherlands and Belgium, as well as the UK.

As a magazine, we have grown significantly since the last issue with new additions the team, along with a whole new website. We have also gone from quarterly to bi-monthly due to demand.

In the coming months we will be adding event reviews, book reviews and a careers section to further expand on our content offering.

I'm grateful for all the people that have contributed to this issue, and I hope you all enjoy the read.

Marc May

WHAT KNOWLEDGE MANAGEMENT CAN LEARN FROM CONSUMER APPS

By Simon Pecovnik,
VP of Product Management at iManage

If you're like most people, at some point over the past couple days, you probably used Google to find an answer to a question – and it's likely that you didn't find the experience to be overwhelming or confusing. You simply plugged in your search terms and a highly relevant set of results appeared, gathered from the vast expanses of the internet.

On the shopping front, you might have used Amazon to effortlessly find the perfect item for your needs. And if you're a music lover, you might have used Spotify to find a specific song to listen to – and, in the process, found recommendations for other great songs you'd like.

The seamless and frictionless experience of these consumer apps – the ease with which they give users exactly what they're looking for – serves to highlight the value of a consumer app-style approach to knowledge management for lawyers.

Room for Improvement

The concept of knowledge management isn't new to the legal industry, but in many organisations, it has historically remained an informal activity – and not necessarily a wholly efficient one either.

Amongst Fortune 500 companies, analyst firm IDC finds that 50 percent of company data is unsearchable, and 30 percent of employee productive time is wasted re-creating existing knowledge assets. It's safe to say that law firms and legal services providers don't fare much better on this front.

While there are numerous challenges in undertaking knowledge management, the biggest one is the fact that data is located in disparate locations – ranging from paper files, to individuals' laptops and internal drives, to more formalised repositories like SharePoint and document management systems.

The net result? While a wealth of intelligence, insight, experience, expertise and knowledge exists in the law firm, it can't be leveraged for meaningful business advantage and client benefit.

It doesn't have to be this way. With the right approach, law firms can make finding this valuable knowledge as easy as finding a piece of information on Google, a product on Amazon, or a song on Spotify.

Unlocking the Knowledge

Let’s say that a fee earner wants to find the very best example of a real estate transfer agreement within the firm to use as a template for a matter they’re working on.

At most firms, this task is not as easy as it seems because even if data has been centralised within a single repository, much of the data is unstructured and thus unsearchable. For all intents and purposes, the various documents are just a bunch of “letters on pages,” and there’s no easy way to tell a real estate transfer agreement from a loan agreement from an employment contract.

Categorising and tagging all of the available documents – in the same way that Google, Amazon, and Spotify have indexed and categorised all of their available items so that you can easily find what you’re looking for – helps bring order to this unstructured data, instantly making it more searchable and valuable for knowledge management purposes. It should be noted here that expecting humans to manually tag and classify all of the available documents isn’t always realistic, so AI is of great use in carrying out this task.

Another thing consumer apps like Google, Amazon, and Spotify do behind the scenes in order to deliver results as effectively as they do is to constantly interpret various signals to make sure they’re delivering up-to-date, relevant results. For example, Google uses a metric like the number of websites that link to a particular article as a “signal” of that article’s usefulness and authoritativeness. Amazon and Spotify use cues of their own to serve up results that they think will be most useful or relevant to you.

Knowledge management works best when it is able to take a similar approach and leverage not just explicit information – like tags, classifications, and other metadata – but also implicit information, like how people interact with the documents and the relationships that exist around the documents.

Making sense of this implicit information – often through AI – helps identify where knowledge lies within the organisation.

For example, looking at the time and billing system and seeing that a particular professional devotes most of their billable hours towards European clients and employment law matters will automatically identify them as an expert in European employment law. Similarly, if a particular European employment law template has been downloaded hundreds of times by dozens of different people throughout the organisation, that's a clear signal that that particular template is one of the best pieces of content for other legal professionals to leverage.

One other thing that consumer apps are very good at is personalisation. The more you use the various consumer apps, the more they get to know you and offer up items that are of the most relevance.

Knowledge management should follow a similar path. Understanding user behaviour – what topics a user has searched for in the past, what files they've clicked on or downloaded, what types of matters they tend to work on, and so on – enables the system to provide richer, deeper, and more precise results to the user over time. As a result, it can offer up results that are most relevant to their daily work, as well as helpful suggestions for other resources they might wish to consult.

The Right Direction

In order to genuinely be successful in knowledge management, a smart, consumer app-style approach to the function is needed. Adopting some of the hallmarks of consumer apps – including frictionless search across all data, behind-the-scenes interpretation and categorisation of that data, and powerful personalization – will be a step in the right direction for any firm that wants to make knowledge management a priority.

About the author

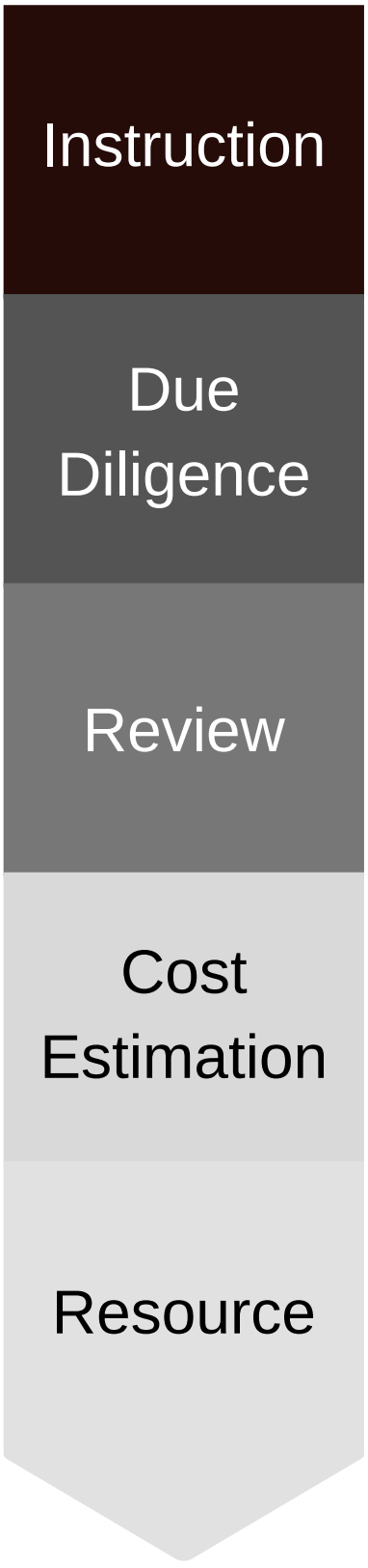
Simon co-founded RAVN Systems and is currently the product manager for iManage Insight. He works closely with iManage customers to understand their needs, provides input on product strategy and manages the planning and design of new capabilities that will transform how professionals work.

Legal Deconstruction

One of the themes for the magazine this year is the deconstruction of legal matters. We believe that one of the skills for future lawyer will be legal project management. As managers they should have the ability to deconstruct the various components of a legal matter and be able to continually make the process as efficient as it can be. In this issue we look at the second element common to all legal matters.

While due diligence has various meanings in a legal context, we will just look at the due diligence required of UK law firms by the regulator, the Solicitors Regulation Authority. This is pervasive of all matters opened by law firms and is aimed at reducing criminal activity, such as money laundering or terrorist financing.

It's important for law firms to ascertain who their clients are, especially if there is no face-to-face meeting. For leading firms this could be as a result of a referral from a foreign firm, or a client that is not domiciled in the UK. Whether there has been a face-to-face meeting or not, law firms are still under an obligation to identify their clients and verify they are not blacklisted or politically exposed.



Law firms' assessment of client risk becomes an exercise in data collection and verification. Those involved with carrying out due diligence will need to gather information on their client's identity if a personal client, and for corporate clients those with significant control over the company need to be identified. They will then determine whether a lawyer within the firm can accept instructions from that client or not.

Assessing clients' credentials is usually done by searching platforms like World-Check, and a human operator is currently required to carry out the search and assess the information received. From experience, the people that carry out this type of work are seen by some lawyers as an obstacle to receiving instructions from their new client.

So how can technology help?

The key benefit will be to speed up the process of due diligence so those in risk roles are able to come to a decision quicker, with the minimum possible impact on the lawyer or their client. Following on from my previous article on instruction it would make sense that the same chat bot functionality could benefit due diligence too. It could ask the client questions and allow them to upload documents without any human

interaction. Through decision tree and workflow (or even artificial intelligence) the information received from the client could be assessed and the appropriate person notified based on risk level. That information could then automatically feed straight into the databases that are usually used to search for client information. This integration could mean that the manual inputting of data is reduced and those risk personnel can assess the relevant information quicker.

If successful, the end result of the workflow would then be that those involved with the matter are notified that they can accept instructions, the matter in the document management system is opened with all uploaded documents added, and a first meeting organised automatically.

I am sure systems like this exist already but perhaps not with the same level of integration or automation. There is a clear benefit in making the process of data collection and assessment as seamless as possible, which makes it as easy as possible for all concerned.

By Marc May
(@doublemarc)

thread

Built with Microsoft Office 365 technology

FOR FUTURE FOCUSED **LAW FIRMS**

Save time with advanced workflow automation.

Collaborate effectively with secure, granular sharing functionality

All of the features your law firm needs:

- ***Time recording***
- ***Billing***
- ***Templates***
- ***Calendar management***
- ***Accounts integration***
- ***Time recording***

www.thread.legal

A day in the deserted life of a legal technologist

By Nicholas Cronjaeger

“OK Nick, so I’ve set you up with 5 RDP sessions here into each of our SQL servers and here are the two Microsoft Access databases, on this USB stick, that we need you to merge into one SQL 2005 compatible version. I need this done within the 60 minutes, so I’ll use our remote VNC software to see where you are up to in about 45 minutes or so. Good Luck!”.

It’s exactly 8 years to the day, that I was thrown into my first foray into legal technology, I can still feel the cheap polyester-mixed suit, shirt and tie combination, drenched in sweat, clinging to my back nervously, as the task of what I had been given to do, entirely overwhelmed me. The gentle whirring of desktop and computer screens accompanied by the acrid smell of soon-to-be overheating black plastic compounds.

To put into context how out of my depth I was, if you’d asked me the week before being thrown into this law firm’s IT department what a relational database was, I would have guessed it was something the government used to see who your parents are.

I am equally thankful that the days of Microsoft Access databases being the source of where our law firms, government and in-house legal departments store their key data has changed, but much still resides on Excel spreadsheets, shared folders, unsecured network directories, unsecured public cloud and yes, you've guessed it, those dreaded USB sticks!

The perception of legal technology has changed, the fears of job replacement are less prevalent, as lawyers, managing partners, CFO's and CEO's acknowledge the immediate need for automation and digitisation within their respective legal functions. The market has reached a level of maturity, that legal technology is shifting from 'nice to have' to 'must have'.

A number of factors have expedited this journey, there certainly were job cuts across the regions in which we operate and government initiatives to be more innovative.
The demand for legal services is still high and growing. As such, lawyers and technologists alike, regardless of sector, are more aware than ever of the solutions available and the need to move quickly.

We now have a small, but growing contingent of legal engineers and legal technologists, working for in-house legal departments, ALSP's and in law firms alike. The clients that I have worked with who have been successful have all taken the approach of 'keeping it simple' and 'making it easy'.

There is a temptation to push for those emerging AI and Blockchain technologies here in our region, but a pulse check on where our clients really are is always required. If you're storing your client confidential data in spreadsheets and shared drives, then let's park those AI discussions for 2019.

My advice

Start with the basics
Keep it simple
Automate effectively
Continue to innovate

As I look forward to the rest of my Sunday, (yes, no matter how long you have been here, working on a Sunday still seems a strange concept), I am reminded of a quote that I would expect resonates for everyone and in particular those engaged in legal services and technology.

"There's a lot of automation that can happen that isn't a replacement of humans but of mind-numbing behavior."

Stewart Butterfield

About Me

Nicholas Cronjaeger is Head of Legal Software Solutions at Thomson Reuters. Operating across the Middle East, Africa, Russia and India, he leads the growth and awareness of all legal software to law firms, corporate legal departments and government sectors.

Help us reach a worldwide audience

Help us provide the best possible legal tech content

Help us inform tomorrow's lawyers

Advertise with us.

How legal tech is enabling law firms to develop new and highly scalable business channels

By Catherine Firmin

Lawyers are artisans. Most of the value they deliver stems from their human capital: decades of experience with a sharp and analytical mind. However, if one leverages almost entirely on human capital, one can only grow new businesses proportionately with expertise and, more likely, time.

Engineers learned a long time ago that by designing easily duplicated machines to take over part of their human capital, they could scale production exponentially while saving time. That saved time could then be set aside for creative work, such as improving those machines (assembly lines, computer program, etc.).

Lawyers certainly also rely on “capital machinery” to make their jobs more efficient: computers, digital assistants and contract management tools. However, this misses an important point: lawyers do not leverage on their skills in typing contracts or managing portfolios to make money. Lawyers rely on legal thinking. Can lawyers then leverage on some technology to do some of this “legal thinking” for them?

The problem with contracts

One of the most time-consuming activities a lawyer performs is document review. Advances in technology such as Natural Language Processing and Machine Learning have certainly precipitated efficiency-driving Artificial Intelligence (AI) tools that can speed up the process. However, many lawyers are still struggling to derive further value from these tools beyond relatively generous time savings. After all, cutting contract review time by half can only double your revenue at most. Herein lies a more fundamental issue in how contractual documents are designed.

The fundamental essence of a contract is still a story-telling narrative. Every contract ever agreed performs the same basic task: it asserts the rights and duties of the parties in a way that can be enforceable should the need arise. However, every lawyer approaches the task of drafting and structuring such contracts in a different manner. The same meaning can be asserted in hundreds of different ways, simply by using different words to say the same thing. This lack of standardisation makes it challenging, even for AI tools, to inter-operate between contract types and is limiting their potential.

The solution with standards

The solution lies in a standard digital contract language: a meanings-based framework that is designed to describe any contract without dictating methods of drafting. This means that drafting differences become irrelevant because the framework is focused on the meaning of the words, and the models infer from different drafting possibilities. One such example is ThoughtRiver's Lexible framework, which is developed by experienced lawyers and leading-edge computational linguists. The framework consists of thousands of data-points that are logically structured much like how a human lawyer would approach contract review. In practice, this framework underpins ThoughtRiver's AI capabilities, which extract critical information from contracts based on the Lexible framework. On top of this, the platform then applies user-customised playbooks to apply a risk interpretation.

Benefits of digital contract language

The ability to develop automated tools against a universal contract language has unlocked exciting new opportunities for lawyers. They are no longer working with tools that benefit only the immediate client project and having to re-invent the wheel each time. They can now simply extend their own module (think specialised contract area), keeping it updated from time to time, and that can be sold on to not only their own client base, but anybody in the community using the same standard. Lawyers would then effectively be codifying their accumulated expertise and building an infinitely replicable machine that delivers value on their behalf. A veritable robotic legal factory.

The market significance of this new channel of delivering legal expertise is phenomenal. Lawyers are creating a predictable and recurring new revenue stream. The technical infrastructure can also be designed such that automated expertise is delivered without giving away any of the lawyer's proprietary design of their "automated review modules". Because any user within the community has access to these modules, law firms can potentially increase their penetration far beyond the industrial and geographical reach that their scale may suggest. It also establishes the law firm as an expert in specific subject matters and serves to entrench an existing market position, as well as open new doors.

Example: Lexible partners

Partners either provide services via the ThoughtRiver platform directly to end-users or provide complementary services to ThoughtRiver customers to support them in configuring the ThoughtRiver platform for their needs. Currently, Taylor Vinters is developing risk playbooks within Lexible for certain contract types.

All of ThoughtRiver's users are then able to use these premium risk policies when reviewing contracts and Taylor Vinters gets commission based on usage. Another use case is how Eversheds Sutherland Ignite is creating and maintaining Lexible modules for the review of contract types that fall under its area of expertise. The firm can almost immediately deploy these modules for automated review of each new client's contracts. It's like having a new service centre that never sleeps.

Although latest research has shown that the legal sector has grown in the past decade, it is more than prudent for law firms to start considering these new revenue streams as alternative providers of legal services exemplified by the Big Four professional services firms' move into the sector. GCs are also leveraging on technology tools to take back work such as contract review. These pressures are already starting to impact the bottom-line. Considerations for implementing the aforementioned new business channels are not purely defensive either. A lawyer with an expertise in any contract area can become a "winner" very quickly and "take almost all" of the market share in that area. As with other digital industries, first movers would have a significant advantage.

For more information please visit www.thoughtriver.com

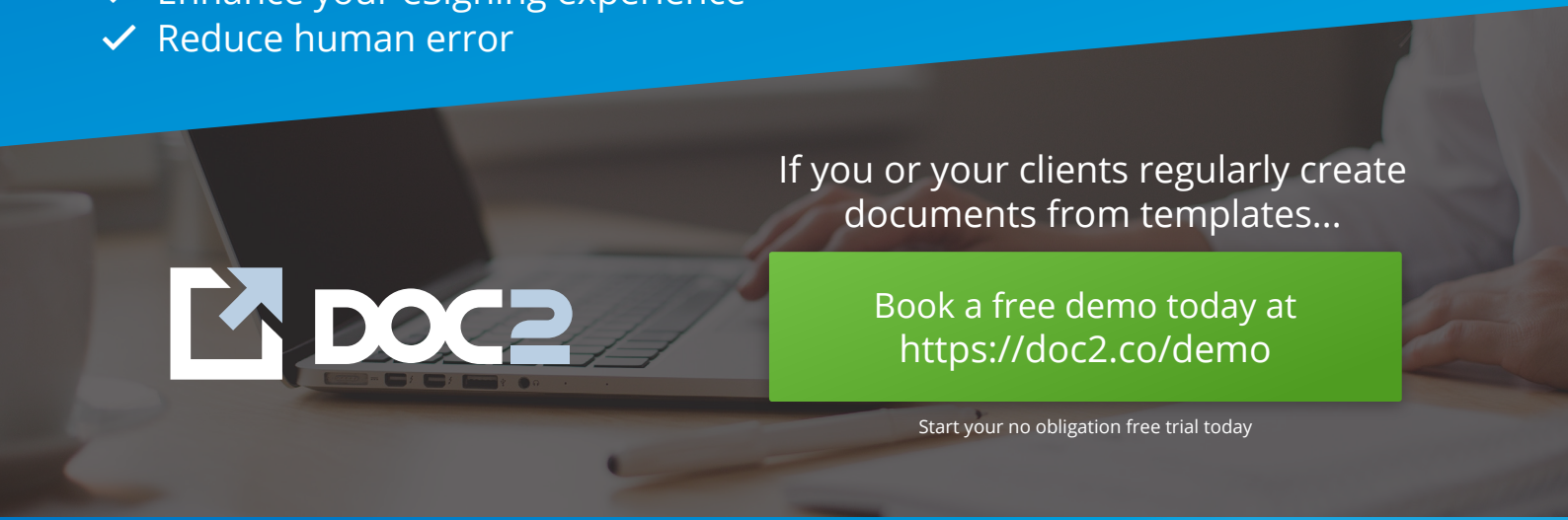
Would you like to contribute to our next issue?

If so, please do get in touch with us at
marc@legaltechnologist.co.uk

Producing documents from templates is so 1999...

Doc2 is an online platform which allows you to create documents faster.
We supercharge your existing templates.

- ✓ No more repeated fields
- ✓ Forget copy and pasting from Companies House
- ✓ Enhance your eSigning experience
- ✓ Reduce human error



If you or your clients regularly create documents from templates...

DOC2

Book a free demo today at https://doc2.co/demo

Start your no obligation free trial today

Who should teach legal tech?

by Caroline Calomme

Training in legal technology is gradually finding its way into law schools, even outside the English-speaking world. Still, we need to remain realistic. No matter how progressive they are, law schools offering these courses are the exception and not the rule. The truth is that the large majority of law graduates start their career without an introduction to legal technology and that very few practising lawyers had a chance to learn about this subject at all during their student years.

This means that, in an average legal department or law firm, probably only a handful of lawyers know what it is about unless they carry out research using their own initiative, i.e. during their "free" time and at their own cost, or they are encouraged to do so by managing partners or a Chief Legal Officer from an older generation. So, wouldn't those organisations be interested in legal tech-savvy hires?

Being against the introduction of legal technology training for students as a matter of principle only makes sense for universities in a few instances. Namely, if the universities believe that students with this knowledge will not be an advantage in the hiring process or that it is not the university's role to improve the employability of their legal graduates. In fact, if it is not the role of law schools to train students in legal practice, why organise moot courts, legal clinics or skill courses? Stressing the need to gain academic skills in law school rather than practical skills could even promote the introduction of a legal technology curriculum, since case law network analysis and other technology-enabled techniques can be powerful research methods.

Beyond the fundamental policy discussion on legal technology education, we must acknowledge that educational institutions face obstacles that the business world may underestimate:

- **Administrative burdens**: How to obtain the required accreditations? How to add a course to the curriculum without having to cancel another one? If it is an optional course, are there enough lecture rooms to welcome the students?

- **Recruitment**: Could a current staff member teach the course(s)? If the decision is made to involve a professor from the computer science or business faculty, how to deal with the interfaculty budgetary hurdles? And, if it is necessary to hire new staff members, what background should (s)he have? Should it be someone from the private sector? How to remunerate them?

- **Content**: While there seems to be an agreement that law schools should not teach how to use legal tech tools as such, what about creating or inventing them? Should it be an introductory course to technology and innovation, leaving it to the students to link this knowledge to their substantive legal courses? Or should it cover key topics in legal technology such as document automation, network analysis, legal design, natural language processing, etc.?

While universities are best suited to impact future generations across all legal professions, we should not forget that in the short term many active legal professionals are still left behind. The hurdles above also show that legal practitioners might to some extent be in a better position than universities to organise training, who are able to focus on content relevant to the market, and most importantly, to the clients that they are serving. It is a tricky argument though because currently most universities leave this task to law firms, which more often than not decide not to invest in the topic.

This is why young generations of lawyers discreetly express the willingness to innovate but are lacking the background knowledge to make a case in front of the more conservative management.

Until more universities and law firms make a move, it would not be surprising to see an increase in companies specialising in legal technology training. They would meet a growing demand for the group of self-learning legal professionals and for the organisations who support this learning track but cannot yet offer a career development track internally.

Who should be trained? How? When? In what specifically? We can host panels, meetings and workshops to argue with each other and get it perfectly right – after all, that is how we were trained. Alternatively, we can try the lean approach and experiment by starting small, using what is already available and collaborating.

For example, my legal tech startup Sket.io works together with the KU Leuven law school in Belgium to teach students how to identify variable and non-variable fields in legal documents and how to draft documents in a computer-friendly format to automate them. Luckily, there are many ways to challenge the status quo:

- Choose a law school with a course on legal technology
- Apply to a law firm with a legal technology strategy
- Invite IT students or your IT team for drinks, coffee or lunch and ask questions about their world
- Partner with legal technology companies or firms with legal technology services to offer internships
- Allow students to enrol in courses at the computer science faculty
- Sign study abroad agreements with universities offering legal tech courses

- Share a list of free online courses and resources on legal technology
- Organise an ideation session, a service design session or a hackathon
- Share a list of free online courses and resources on legal technology
- Explain useful legal concepts to developers in exchange for a basic introduction to programming

As a final thought, the decision to train or not to train (future) lawyers should perhaps not entirely be up to universities and the private sector. Do we really want a society where professional qualifications to protect and defend legal rights are awarded without guaranteeing sufficient awareness of the available technological solutions? Without this knowledge, it could be difficult to act in the best interest of your clients, a fiduciary obligation in the legal profession.

By Caroline Calomme (@CarolineCalomme), Brussels Legal Hackers community founder & Sket.io co-founder.

Blockchain and Cybercrime

An interview with Chris Recker

By Myat Eaindra Cho

Chris Recker, an associate specialising in commercial litigation and civil fraud at Trowers & Hamlins has given us his expert insights into the world of blockchain and cybercrime. Trowers & Hamlins is an international law firm with offices throughout the UK, Middle East and Far East.

What made you choose cybercrime?

Because of the civil fraud work that I do. 70% of all fraud is cyber, according to Action Fraud UK. This means that more and more of the work we do has a cyber and tech angle to it, so I was drawn to this challenging and emerging area. I've got to work with some great cyber security companies which deal with pretty unusual and fast paced challenges that organisations have had. Cyber security is a very real risk so being ahead of the curve is important.

What do you think are the main challenges of combatting cyber crime?

Technology is ultimately an enabler for fraud and cybercrime. Whilst technology allows organisations to innovate and actually reach customers which they wouldn't ordinarily be able to reach, it also allows people (fraudsters) to change their online identities, their IP addresses, thereby changing their locations, and manipulate information that's available on the internet. The risk of being caught is considerably lower than the risk of literally robbing someone on the street.

The biggest challenge is often the 'human element'. If your people aren't trained properly, they can be the breakdown in the protocol. They are the ones subject to social engineering, and they are the ones who are sent the phishing emails (for example). The challenge is that fraudsters are trying to get access to data (held by both individuals and organisations) so are often looking at new and innovative ways to manipulate individuals and bypass security protocols.

One of the other challenges relates to the prospects of recovering misappropriated money or assets following a cybercrime incident. However, following on from *CMOC v Persons Unknown* the court has reiterated (*World Proteins v Persons Unknown*) that freezing injunctions can be obtained against unknown parties following a cyber fraud incident. This will really help victims of cybercrime to trace and restrain those funds or assets.

What would you say are the opportunities for blockchain in combating cybercrime?

There are opportunities for blockchain technology to help combat fraud and cybercrime. One of the biggest benefits of using

blockchain is the distributed ledger technology. This ultimately means that the control of the ledger is spread across many individuals.

The significance of that is that it is very difficult to amend the ledger. Some people say that what you have is a 'tamper-proof' system. Blockchain technology is not set up in a way that encourages people to illicitly amend the ledgers because there is no benefit to them for doing so (as the benefit of any mining, if it is a cryptocurrency ledger, is only rewarded if an amendment to the ledger is actually accepted). As a result, blockchain technology avoids the 'single point of attack' that hackers could ordinarily take if they were looking to attack a specific piece of software or hardware.

There are also opportunities in specific sectors, such as the supply chain sector, where there is a need to trace goods to their originating source.

Do you think blockchain can prevent cybercrime?

In certain sectors, it will be particularly useful. However, it is not the complete answer. We are not yet at a stage where information can be added to a blockchain without human interaction. Therefore, it still requires the person entering the information to be honest when doing so. Blockchain, therefore, cannot erase corruption (if, for example, all members of a private blockchain agree to alter a ledger).

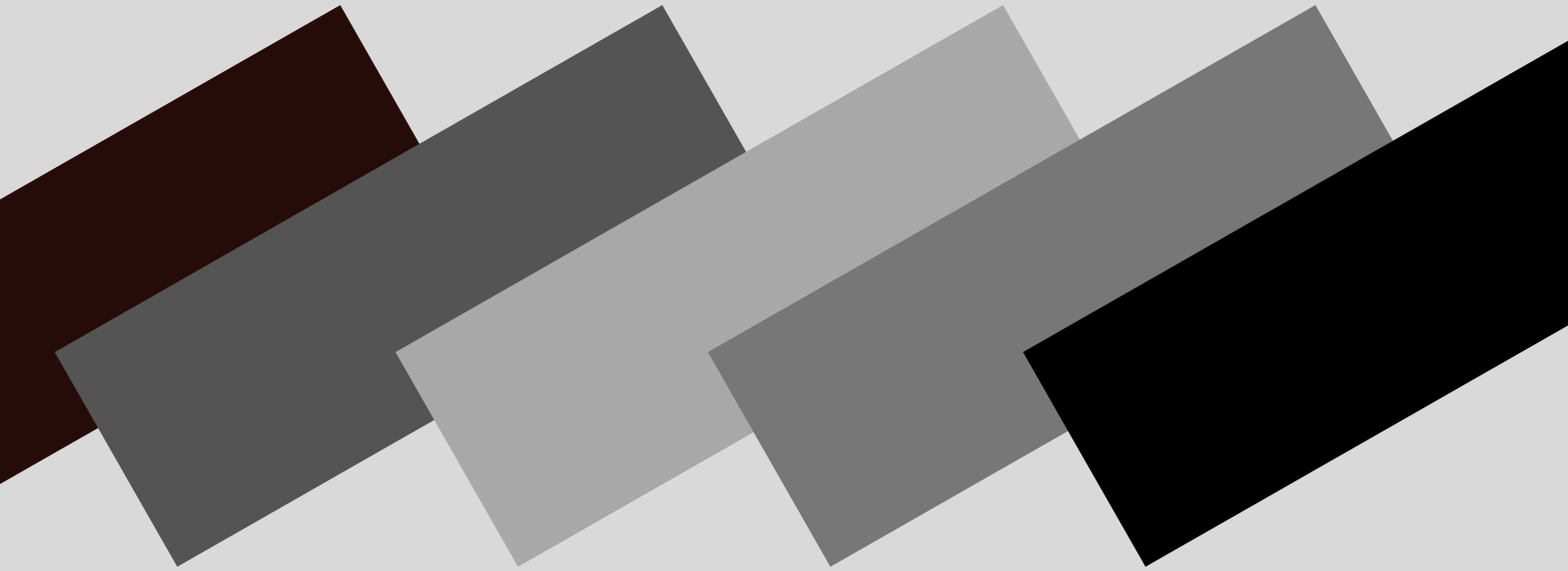
Blockchain is a step in the right direction, but it is not the complete solution to cyber risks.

How can firms and businesses best protect themselves from cybercrime?

Prevention is the best cure. It’s about having a solid risk management framework of your people, processes and technology. This involves having a response plan, knowing who you’re going to go to if there is an incident, and keeping your perimeters guarded. It also requires carrying out a risk assessment and knowing who your experts are. This will put you in the best place to respond. This won’t be able to prevent it completely, but it will help when you are liaising with a regulator and showing that you have acted reasonably.

So, preparation is key. This includes involving the relevant experts (including cyber, legal and PR) and following your plan. The sooner the legal team are involved, the sooner the documents can be made confidential using legal professional privilege for any investigation.

Thanks for your time Chris.



E-Commerce, Cyber-Security and Governance in Africa

By Alice Namuli Blazevic

Technology is at the forefront of our growth as a continent. Africa has witnessed phenomenal growth in the ICT sector in the past decades; internet use statistics indicate that Africa's population of Internet users grew from about four and a half million people in 2000 to about 400 million people in December 2017.

We are experiencing exponential growth in e commerce driven by the high tech start-up scene on the continent, changing the way we live and do business. In spite of debates about its 'Africanness', the listing of the e-commerce start-up Jumia on the New York Stock Exchange proves that African markets aggregated by technology is as an attractive target for capital investment as any around the world. The e-commerce industry in Africa is also expected to expand to USD75bn by 2025. Meanwhile, fintech pioneers like M-Pesa (mobile money) and Bitpesa (blockchain-backed transfers) are moving enormous sums of money across the continent at very low costs.

However, the growth of e-commerce and the more people access data or the internet in Africa, the more concerns arise over misuse of the internet and the need to promote cybersecurity governance on the continent.

On an annual basis, we experience hundreds of millions of sophisticated cyber attacks on the continent. The market is saturated with cyber-hackers, who are adept at deploying the latest weaponised vulnerabilities in order to access valuable data for ransom, fraud, theft from financial institutions, governments to private companies. Many cyber security practitioners have warned that if the current statistics continue to grow, combined with the absence of a collaborative and strong defensive cyber mechanisms in place, cyber attacks have a high potential to cripple African economies.

The most recent cyber-attack on the continent took place on 3rd June 2019, when 18 Kenyan government websites were hacked. Luckily, according to the Kenyan authorities there was no critical data compromised. But it is worth noting that the number of cyber threats identified by Kenya’s government in the first quarter of 2019 almost tripled to 10.2m from the previous year. It is fortunate that the 18 hacked sites did not compromise citizen or national security data, but it is easy to imagine that new attacks will succeed to do so.

Such incidents can’t be ignored and they raise obvious questions. How prepared are African governments for cyber attacks?

According to the Global Cyber Security Index of the International Telecommunications Union, the African continent is performing poorly with the lowest level of commitment to cyber security found in its ranking.

Below is a breakdown of key statistics for most affected African countries:

Many African countries have no specific cyber legislation, for the few countries where cyber laws exist there is no strict adherence and there is a general lack of awareness of cyber security measures resulting in a conducive environment for cybercrime in Africa.

So far, 21 African countries including, Angola, Benin, Burkina Faso, Chad, Equatorial Guinea, Mali, Gabon, Ghana, Ivory Coast, Lesotho, Madagascar, Malawi, Morocco, Niger, Senegal, South Africa, Tunisia, Zambia, and Uganda have enacted data protection and privacy laws. And 5 countries have laws in draft stages (including Kenya, Nigeria, Togo, Tanzania and Zimbabwe).

Uganda, for example, has a number of legislations in place which address internet misuse and these include: The Data Protection and Privacy Act 2019, The Computer Misuse Act, The Electronic Signatures Act, The Electronic Transactions Act, The Access to

Information Act and The Regulation of interception of communications Act.

Uganda's 2019 Data Protection and Privacy Act was benchmarked on the EU data protection regulations and has similar clauses to GDPR which require strict compliance. All data collectors are required to obtain consent from data subjects, and notify the regulator in case of any breach. For failure to comply or if found in breach of the law, the maximum penalty for companies is 2% of their annual gross earnings. For individuals, the fine is about USD 1280 and/or 10 years' term of imprisonment.

Regionally, there are efforts to ensure data protection within regional blocs. For example, the Southern African Development Community (SADC) has developed a model law harmonising policies for the ICT Market in Sub Saharan Africa, which includes components on data protection. The Economic Community of West African States (ECOWAS) has created the Supplementary Act A/SA.1/01/10 on Personal Data Protection within ECOWAS. And several Francophone countries (Benin, Burkina Faso, Ivory Coast, Gabon, Mali, Morocco, Senegal and Tunisia) are part of the French-Speaking Association of Personal Data Protection Authorities (AFAPDP) which promotes personal data protection principles and rules in French-speaking countries.

The African Union imposes obligations on member states to establish legal, policy and regulatory measures to promote cybersecurity governance and cybercrime through its regional cybersecurity treaty, known as the Convention of the African Union on Cybersecurity and Personal Data, passed in June 2014.

It convers a broad range of issues, including but not limited to e-commerce, data protection, cybercrime and national cybersecurity.

However, so far, only ten African countries (Benin, Chad, Comoros, Congo, Ghana, Guinea-Bissau, Mauritania, Sierra Leone, Sao Tome & Principe and Zambia) have signed the convention and only two (Mauritius and Senegal) have ratified the convention.

Once a member states ratifies the convention, it is required to enact personal data protection laws as well as develop a national cybersecurity strategy, pass cybercrime laws, and ensure that e-commerce is exercised freely.

The adoption of the AU Cyber Security Convention underscores Africa's efforts to promote cybersecurity and governance on the continent.

In spite of this progress, it is clear that additional investment in ICT and cybersecurity literacy, infrastructure development in both the public and the private sector, collaboration of African governments, enforcement and strict compliance of existing laws, as well as a shift towards a cybersecurity mind-set is needed to give force to the incipient legal framework on the continent.

About me

Alice Namuli Blazevic is a Partner with Katende, Ssempebwa & Co based in Uganda. She specialises in Technology Law with a keen interest in Blockchain, Crypto currencies, Fintech and Artificial Intelligence.

THE PRACTICAL STEPS FOR YOUNG LAWYERS TO MITIGATE CYBER THREATS

By Motunrayo Akinyemi

The advancement in the use of technology in the corporate world suggests the need for all professionals especially lawyers, law firms and the entire legal industry to protect itself against increasing cyber threats and evolving cybersecurity landscape. The legal industry is not immune from cyber-attacks. Therefore, it is important for lawyers to identify and document asset vulnerabilities by answering these questions:

What makes our practice attractive to cyber criminals?
What information do we obtain from the client?
How is this information stored?
Who has access to this information?

From the foregoing, it is right to state that lawyers do utilise and keep highly sensitive and confidential information of their clients such as names, email addresses, home addresses, business secret, details of transactions and other sensitive information. Consequently, lawyers and law firms have become prime targets to cyber attackers who want to steal this information for their dubious use.

According to the Ponemon Institute Report 2017, the average cost of data breaches incurred by organisations increased from $3.62 Million in 2016 to $3.86 Million in 2017. The key factors for the increase in cost were found to be; security automation and the extended use of Internet of Things (IoT) devices. From the reports, it is evident that organisations need to double their efforts in protecting their important assets.

How can lawyers protect themselves from cyber risk?

MITIGATING CYBER RISKS/THREATS.

The use of security mechanisms: Users should install Endpoint Protection Software (anti-virus, anti-spyware, user-based firewall, anti-malware,) and intrusion detection/ intrusion preventive systems.

Firewall: The firewall acts as a protective layer between the user and the internet with the duty of tracking and analysing data exchanged between the computer and the server. Ensure the firewall on desktops/laptops are switched on to prevent unauthorised access.

Password Management: Users should establish strong passwords on all devices, create different passwords on various websites, and for practical guidance, passwords should include; numbers, upper and lower case letters, symbols and so on. For ease, users should download password manager softwares such as 1password and LastPass. Also, it is advised that users desist from automatic log-on functionality, change default passwords, and desist from storing password using weak encryption or hashing algorithms.

Public Wi-Fi: Users should avoid the use of public internet access. An unsecured WI-Fi connection is susceptible to threats as hackers can use it to distribute malware or launch a man-in-the-middle attack. If a user intends to connect to an unsecured Wi-Fi connection, the user could; make use of a virtual private network (VPN), ensure that every connection initiated to a web server is secured by a TLS/SSL connection, turn off the sharing option, and turn off the Wi-Fi when it is not needed.

Social Engineering: This is a common psychological manipulation technique used by cyber attackers to trick innocent users into handing over confidential or sensitive information. It is advised that all personal identifiable information is not unnecessarily disclosed online. For example, answers to secret questions such as mother's maiden name should not be stated except during the initial registration on a secured website. Other techniques used are phishing mails appearing to be from a bank, pretexting and false court notice to appear etc.

Data Encryption: This is the conversion of data from a readable format into a coded form that can only be read or processed after decryption. The use of encryption will guarantee safety of the user's information sent between a browser and a server such information include; Personal Identifiable Information (PII), payment data information and so on. Therefore, the use of encrypted mail service such as ProtonMail, and file sharing will be advised. In the event where a user cannot access encrypted email or file sharing device, files should be zipped with a password.

Software Updates: Users should update the software on their devices regularly because these updates usually fix or eradicate computer bugs, prevent the spread of viruses on other devices, protects data on the device, and patch security vulnerabilities.

Cyber Training: Users are advised to read up on cyber updates on latest threats, educate and train employees on how to avoid risks. Also, treat suspicious emails and unknown client inquiries. For example, ensure attachments from suspicious emails are not downloaded to the desktop/personal computers.

Incident Management: This involves the management of cyber risk which could be done by in-house expertise or by 3rd party experts who carry out forensic investigations in the event that a breach occurs. It is extremely crucial that the plan is approved by the management of the firm and they are also carried along when consequential changes are done to the said plan. The incident response plan should contain the following:

a. Identification of the asset to be protected;

b. Identification and allocation of responsibilities in the event of a cyber security incident;

c. Engage 3rd party experts or in house expertise for incident response / forensic investigations in case of a cyber breach incident;

d. The equipment and technology to detect and address a cyber security breach;

e. Containment strategy by disconnecting systems immediately or collect evidence against the cyber attacker who perpetrated the system;

f. Communication strategy for internal and external stakeholders and law enforcement agencies.

In conclusion, it is critical to note that total prevention from cyber-attacks is impossible and it is the duty of stakeholders in the legal industry to take a risk based approach to ensure protection and mitigation of threats. The industry regulators should create standards and cybersecurity guidelines. It is also advised that

lawyers purchase cyber-liability insurance or engage technology vendors who offer cyber insurance to cover liabilities in the event of a breach. It is crucial to have a cybersecurity policy and hygiene well immersed into operations and all layers of their organogram. Finally, law firms can prepare an incident response plan in the event that the inevitable occurs to prevent irretrievable loss of assets.

Motunrayo Akinyemi
Lagos,
Nigeria.

Competition law should prevail over intellectual property rights

by Roderik Plukker and Birgit Verbeek

Roderik and Birgit are both LLM students at the University of Utrecht in the Netherlands.

Introduction

The "new economy" is up and rising, which means that innovation is more important than ever. In this new economy it is not so much competition within a market, but more competition for the market. "Killer apps" can take over markets, or create new ones, in no time. A consequence of this is that intellectual property rights (IPRs) could once again be at the centre of discussion regarding its conflict with competition law. In this article, we will discuss the question "should competition law prevail over intellectual property?" Our focus will lie in Europe, and thus we will study European Union laws and markets. To find an answer to our research question, firstly, we will discuss the objectives of both competition and IP law, and the relationship between the two. Furthermore, we will give an example that shows the challenges that arise with these conflicting systems. Thirdly, we will discuss the needed balance between compulsory dealing and protecting innovation, using European case law to showcase the importance to the European Union. Finally, we will conclude with a clear judgement with regards to the research question.

The relationship between competition and IP law

Competition law is part of the EU law framework and contained in the Treaty on the Functioning of the European Union (TFEU). IPRs are generally governed by national law. Foremost, IPRs are seen as necessary incentives for investment in R&D and innovation because they offer theprospect of a reward for the investment and decreases the risk of devaluation by free riders. It also allows the owner of the IPR right to regain investments at a higher level than would have been possible in a fully competitive market and licensing enables exploitation in instances where the inventor does not have the means to do so itself. Copyright protection allows content creators a chance to earn an income with their work.

IPRs protect exclusivity whereas competition law strives to keep markets open. The former can be considered anti-competitive because they can restrain other firms from benefiting from the innovation without the consent of the holder; hence they can constitute barriers to entry and create market power in absence of substitutes. The Technology Transfer Guidelines, on the other hand, state that both bodies of law have the same objectives, namely promoting consumer welfare and an efficient allocation of resources, and that innovation constitutes “an essential and dynamic component of an open and competitive market economy”. IPRs can stimulate investments in innovations which lead to a more competitive market. These investments would not be worthwhile without patent protection.

Treaties do not affect the existence of IPRs, but their exercise may be restricted by EU law. However, only where the exercise is associated with a practice which is unlawful under Article 101 or 102, will the exercise of an IPR be limited by competition law. A license does not infringe Article 101(1) TFEU unless it contains

restrictions that have the object or effect of restricting competition. Licensing agreements can be seen as beneficial, especially when the licensor and licensee are not competitors, because they introduce a new competitor into the market and help diffuse the invention throughout the economy. Similarly, in an economic sense, an undertaking does not necessarily become a monopolist when possessing a patent; as long as there are adequate substitutes they do not confer market power. In the AstraZeneca case, the General Court stated that “The mere possession by an undertaking of an exclusive right normally results in keeping competitors away, since public regulations require them to respect that exclusive right”. Article 102 TFEU may apply in case of an improper exercise of an IPR. For an infringement to be found, the exercise of the IPR must be linked to an unlawful practice such as illustrated in Hoffman La Roche where the court stated that the IPR must be used as an “instrument of abuse” of a dominant position.

Commissioner for competition, Margrethe Vestager, said in a speech that competition law may complement IP law in situations where the exercise of IP law may fall short of promoting consumer welfare. Steven Anderman has gone as far as to argue that an extra tier of regulation is added by competition law to the already existing IPR regulation.

The conflict in practice: Cross-border audio-visual services

Copyright is granted under national laws and is confined to the territory of the Member State in scope and effect. This is called the principle of territoriality. The principle implies that any aspect that has not been harmonised at the EU level is governed by national law. Due to the territorial delimitation of IPRs, they cause a conflict with the internal market. An example of such a conflict is the (lack of) provision of cross-border audio-visual services within the internal market. IPRs can be used in ways which compartmentalise the internal market.

The requirement of a separate licence in every Member State where the copyrighted work will be exploited inhibits the free movement of goods and services. Consequently, cross-border competition for these audio-visual services is restrained.

A territorial exclusivity clause in a license does not infringe Article 101(1) per se; this is dependent on its effect on the market. However, clauses granting absolute territorial protection against any form of intra-technology competition will nearly certainly be an infringement of Article 101(1).

The Court reached this conclusion in Consten and Grundig. Yet, in Coditel v Ciné Vog Films the Court decided that the contractual territorial exclusivity did not infringe Article 101(1) due to the special circumstances of a performance copyright. It took into account the characteristics of the cinematographic industry, which it found to show that the exclusive exhibition licence did not in itself prevent, restrict or distort competition. In Premier League, where the court also took into consideration an additional obligation, the prohibition to export decoding devices, and concluded that there was in fact a restriction of competition by object. The court found a restriction by object because the licencing agreement obliged the "broadcaster not to supply decoding devices enabling access to that right holder's protected subject-matter with a view to their use outside the territory covered by that licence agreement".

The majority of geo-blocking measures is raised by non-dominant sellers making unilateral decisions. The scope of application of competition law in this area is therefore limited to the 12% of measures which are a consequence of contractual agreements. The Pay-TV investigation illustrates the application of competition law to licencing agreements. In 2014, the EC initiated formal proceedings against a number of major US studios because of their licencing agreements with EU broadcasters, which it

suspected were a breach of Article 101 TFEU. The proceedings focused on the clauses which gave “absolute territorial exclusivity and hence compartmentalised the market and eliminated cross-border competition between pay-TV broadcasters.

If competition law prevails over IP law, it can be used as a means to an end and secure competition in IP-heavy markets such as the audio-visuals services market. However, banning exclusivity as a whole would be undesirable because the license clauses are often a consequence of the characteristics of the industry rather than a breach of Article 101(1), as the Court also concluded in Coditel.

Balancing interests: compulsory dealing versus protecting innovation

In this paragraph we will examine the stance the European courts have on the balance between compulsory dealing versus protecting innovation, starting in the first major case where these two interests stood directly against each other; Volvo v. Veng. In these cases, the European courts "unbundle" complex goods which makes it easier to establish dominance in a certain market, which has been met with criticism.

Volvo held the sole design rights over front wing panels, which led to them having a monopoly. Veng, who imported the parts without Volvo’s consent, infringed Volvo’s IPRs by doing this, which led to Volvo starting a lawsuit. In this case the main question was: is it prima facie abuse of dominance to refuse a license? The court ruled that it was not since this since the ability to prevent third parties from manufacturing/importing protected designs was the central matter of these IPRs. However, if certain "exceptional circumstances" arise, it can be seen as a refusal to deal, and thus abusive.

Then came the Magill TV Guide case. In this case the European Commission established a few circumstances which can be seen as the aforementioned "exceptional circumstances". Here Magill held IPRs on their weekly TV guides. However according to the Commission there we no real substitutional goods, and most importantly, the IPRs stopped the emergence of a new product. Especially this last factor was of importance to the Commission, and which led them to order Magill to license their product.

Then followed the IMS Health Inc. v. Commission case. In this case the court broadened the circumstances when refusal to deal can be seen as abusive, it introduced the "essential facility test". This test entails that when an IPRs holder has a de facto monopoly, and leverages this position on a downstream market, where its product is seen as an "essential facility/input", abuse can be established. IMS created a "brick" structure for displaying sales data, which became the standard within the market, and thus essential since it was not economical for secondary market producers to produce it. And so, IMS was ordered to license their brick structure.

Then came possibly the most important case in this field of law, the Microsoft case. Microsoft refused to share information concerning their operating systems. This prevented other producers from producing operating systems capable of interoperating with Windows computers. Microsoft said the refusal to share this information was because it had the intention to innovate. The court, however, disagreed. The "new product" rule was dropped, and the court found that when a refusal to deal can have an effect on possible innovation, abuse is established. In this case, other producers needed the information in order to innovate, so unlike Microsoft reasoned, the court said that the information was of such importance that the refusal to share actually slowed down innovation. This was a major breakthrough since the

circumstances that make a refusal to deal abusive were broadened even more. A "possible impact on innovation" is now enough to establish abuse.

As showcased in the previous cases, the EU is broadening its understanding of "abuse", and competition is prevailing more and more. This is perhaps to be explained by the fact that competition law is at the centre of European law where IP law is mostly regulated by the member states. Especially with the Microsoft case, the EU established the doctrine that IPRs can actually have a negative effect on innovation, which makes the refusal to deal abusive.

Conclusion

IPRs can stimulate innovation. However, it comes at a price. As discussed above, IPRs bring the risk of inhibiting competition within the internal market. A good example of this is in the area of cross-border audio-visual services. Here it showed that it can also be detrimental to the free movement of goods and services. Competition law does not (yet) always prevail over intellectual property due to the specific subject matter of the latter and characteristics of, for example, the audio-visual industry. However, with the Pay-TV Investigation, the Commission has shown intent to utilise competition law to regulate IPRs. Furthermore, following the discussed cases, especially the Microsoft case, the EU shows the tendency to let competition law prevail over IPRs. We feel that this is a good course to take, at least until IPRs are further harmonised to make sure the markets are stable, and the consumers rights are protected.

By Roderik Plukker and Birgit Verbeek

Why law firms need to innovate (or else..!)

By Steven O'Donnell

A story like this one would have once been a jarring exception in the annals of corporate client-outside counsel relationships.

But nowadays? It's nearly old news: Teva Pharmaceutical's CLO, David Stark, has decided to slash the number of outside law firms handling his business. His primary goal? Significant discounts, which he sees as something he can obtain from "hungry" firms. In his mind, he's not seeing sufficient value at the rates being charged by many of the rest.

He's quoted – 'disapprovingly' – on how "growth rates of law firms are far exceeding the growth rates of the pharmaceutical industry."

What he's doing is not an isolated instance. In-house legal departments, CLOs and GCs and their staffs are under ever-tightening pressure to do more with the same – or even less – in terms of budgets and resources. That pressure, naturally, is passed along to law firms.

More pressure from multiple directions

Legal “consumers,” both corporate and individual, are more informed about what they’re paying law firms, and what they’re getting out of it. They’re forcing new billing models, but they’re also implementing e-Billing and financial management technologies to manage the challenges of controlling legal spend and maximizing value received.

Until the global financial crisis of a decade ago, there were few pressures on the legal industry (or some others) to change. Law firms could cut internal costs rather than invest in innovation, and lawyers have a historical aversion to adopting new practices anyway.

Today, however, law firms are being forced to transform themselves or perish. Client pressure is not the only factor at work; competition – from other firms and alternative service providers – is very real, and even the judicial system is getting into the act, as judges press companies (and, by implication, their law firms) to utilise technology tools to do a better job in areas like collecting and collating e-discovery and legal hold data.

In an instance like Teva Pharmaceuticals, a law firm is faced with blunt choices. It can innovate by making itself more efficient and agile in order to deliver a high level of service while still maintaining profitability, stand pat and endure shrinking billings and margins, or wave goodbye to that client in hope of finding another who’s satisfied with the “traditional” paradigm. The first is technologically feasible; the second is risky and difficult; the third is wishful thinking and incredibly expensive, since it costs a firm 10x more to obtain a new client than retain an existing one.

Technology offers innovation tools that can make law firms

more competitive, responsive, and efficient. But any tech tool, or suite of technologies, isn't enough. To leverage them effectively, there are three key pillars that must be in place:

1. Be bold

Having the courage to move forward is vital. As Stephen Embry and others have noted, law firms haven't felt much heat to evolve until recently. But entities like CLOC, already driving the Legal Operations movement for in-house legal departments, are now extending opportunities to law firms to become part of the "ecosystem" of innovation and collaboration that have already manifested results in Legal Ops.

Solutions like SaaS workflow automation are relatively easy to adopt and use and can reward law firms with "quick wins" that make further technology adoption more palatable. Digitising and automating the processes underlying legal services renders them standardised and efficient, which rewards the law firm's initial courage with bottom-line results.

2. Embrace co-innovation

One strength of technological innovation? How it creates opportunities for co-innovation, where law firms can build internal forums for sharing ideas, or even become partners in that "ecosystem" I mentioned, which includes clients and service/technology providers, where not only platforms and services are shared, but ideas and collaborations.

Some law firms have even taken the lead in building these ecosystems on behalf of their clients, rather than waiting for clients to force innovation on them. Keesal, Young & Logan have partnered with Mitratech in a Keesal Propulsion Labs initiative through which they advocate for the creation of "legal service centers" within client companies, serving as enterprise

transformation centers where Keesal can help clients ensure legal and compliance best practices are "*intertwined throughout existing processes at the start and middle, rather than just the end*" as KYL's CIO/CISO, Justin Hectus, has explained.

In our own case, we've launched a TAP Co-Innovation Center where users of our own workflow automation solution – law firms included – can share workflow designs and ideas. It's a service that's been roundly embraced by our user base, and that's another indicator of the sea-change in attitudes that's happening in the industry.

3. Empower the right people

The courage to change and a willingness to co-innovate are futile without having the right people in place to move innovation forward. They're as important as any technology asset, maybe more so.

The human factor is obviously central to everyday operations, and it's even more key to making innovation a reality. People with a willingness to push modernization forward should be complemented by processes, assigned roles, and a set of goals that allow them to institute the kind of positive changes that can give a law firm a reputation for efficiency, agility, and client-centric innovation. That reputation is a yardstick that more clients than ever are applying in evaluating outside counsel.

Steven O'Donnell is Head of Product Marketing - Legal Operations at Mitratech. He has a wealth of knowledge and experience about the challenges facing legal professionals. A regular speaker at industry events and webinars, he provides in-depth insight into how technology is transforming the legal industry.

Past editions

If you would like to have a read of our previous editions please click on the links below:

- May/June 2018 Issue

- October 2018 Issue

- January 2019 Issue

- March 2019 Issue

Next edition

Next edition will be out in August 2019.