Business Insights in Trade Secret Management

The Trade secrets, the smartcard and the hacker

Christine Maury Panis
Former EVP General Counsel and Public Affairs
Consultant

Company and Sector Specificities

1. **Can you briefly describe your business and to what extent the protection of trade secrets is a crucial issue for you?**

I have spent the last 23 years as EVP, General Counsel and Public Affairs at an affiliate of a major telecom company in France (the Company).

Presentation of the Company

Bringing video and security together for over two decades, the Company provides premium TV platforms, OTT ("Over- the- Top", it encompasses TV services that are going over the top of the established broadcast companies to reach consumers with content. OTT is a catch all-term for various types of streaming video services that use the internet or mobile phone networks to directly deliver content to the viewer) and content protection to TV operators, broadcasters and content providers around the world.

The Company's solutions have been deployed globally at over 100 customers in more than 35 countries. With headquarters based in Europe and offices around the world, in Finland, Hong-Kong, in the USA, Mexico, Argentina, Chile, Malysia, Singapore, Miami, Dubai, Tel- Aviv, the Company has recently expanded into the world of Targeted TV Advertising, Anti-Piracy solutions and in the industrial 3D printing space, where it helps securing Industry 4.0 platforms. Industry 4.0 refers to the revolution that transforms manufacturing, design and operations by combining digital and physical technologies. It enables new business models and organizational structures, for instance in the 3D printing it allows certain industries to create customized parts on demand without needing inventory or warehousing.

The Company used to have around 400 employees worldwide and had an average turnover ranging between 75 and 100M Euros. In order to understand the challenges of the Company around trade secrets, I shall make below a brief history of the Company over the last 25 years and focus on its early days when it was mainly dealing with content protection.

FROM THE CAS" SOLUTIONS TO WATERMARKING AND TO THE 3D PRINTING CHAINS

The Company started in the Conditional Access systems (CAS). A CAS solution is a hardware and software based solution that protects contents, it is used by Pay TV operators and providers (such as CANAL + in France, BSKYB in the UK) or by streaming platforms desirous to make their content, especially their video premium content like recent films or sport events available to these of the customers (subscribers) having paid a subscription in that respect.

CAS is an essential element of security that determines who is allowed to access certain data, apps, and resources and in what circumstances.

A CAS is actually a combination of trade secrets ; these secrets encompass (i) the cryptographic encryption keys used by the pay tv provider to encrypt its signals, (ii) the

decryption keys located in the decoder and in the smartcard that is inserted into the decoder,(iii) proprietary algorithms and protected electronics and computer codes inside the decoder and the smartcard, both serving as safes for these algorithms and codes (all these elements being referred to as **"the Trade Secrets")**. On top of these standard features and in order to strengthen security, the smartcards delivered by the Company contained additional secret keys. In that respect, the Company used to organise what it called the "**Secret Ceremony**". This "Harry Potter" like sounding title meant completing personalization of the smartcard by adding a secret to make it unique to a given Pay TV operator. The customer came at the Company's location and both Company and customer jointly generated dedicated cryptographic keys. These additional cryptographic keys were then inserted on a dedicated cryptographic card, such card was put in an envelope, I used as the General Counsel to seal the envelope and such envelope was kept in a safe at a bank.

IMPORTANCE OF TRADE SECRETS

Trade Secrets have therefore been the core of the business. They were all the more critical in terms of the related investments needed, the revenues, the competitive environments and the related hacking practises.

The costs involved

Maintaining and enhancing these Trade Secrets meant huge investments. In the days of the smartcard, the Company had to develop every two years a new smartcard, not meaning that the card duration would be two years but just in case of a hack. These costs were in million Euros.

The revenues involved

In terms of the Pay TV, the revenues of business based on CAS has been sharpy falling, which is principally due to new modes of content consumption but also largely due to the new forms of piracy, i.e., illegal streaming. The business has been however extremely flourishing, global pay TV revenue peaked in 2016 at USD 201 billion but then began to decrease year on year and dropped to roughly 151 billion U.S. dollars in 2022. It is expected that by 2028, worldwide pay TV revenue will have fallen by around another 26 million U.S. dollars.

CAS COMPETITIVE ENVIRONMENT, DISTORTED PRACTISES AND CONSOLIDATION

The Company's environment was highly competitive and sensitive. In the early days of CAS, in Europe, only 5 companies were able to provide CAS systems to Pay TV operators in Europe. When CAS used the smartcard, competition was fierce as it was known that smartcards could be - depending on the robustness of the Trade Secrets and the strength of the technology involved – be more or less easily hacked. For a hacker, hacking has always been a question of time and money as no CAS is completely secure. In our industry, no company would ever give any warranty as to the longevity of a CAS.

Each time a smartcard was hacked, it was a difficult period. At a first glance, one might think that CAS providers would benefit from a hack as they would have the opportunity to sell millions of new replacement smartcards to their customers to reinitiate the security of their system. Actually, the situation was very different. Due to the immense costs, each time a Pay TV operator had to buy new replacing smartcards, it used to launch a new tender, meaning that the current CAS supplier was always at risk a losing a major customer.

Before the shift to illegal streaming, smartcards used to last four to five years. As of the fourth year following the introduction of a new version of smartcard, the risk of successful hacking grew and often you could see very first publications of hackers claiming that they hacked the

Trade Secrets withing the smartcard. As an ultimate phase the code of the smartcard was disclosed on the internet. At that time the smartcard was compromised, and it was clear that a change of the smartcard needed to be seriously considered to maintain security.

In this context, certain external software companies using this context had even specialized in "card swaps" and offered their services to Pay TV operators, claiming and pretending to have intrinsic knowledge of existing CAS systems and proposing robustness assessments. These assessments posed risks, as they required exposing Trade Secrets to "external" auditors who, despite confidentiality commitments, could retain much information in their “unaided memory”. This trend came in connection with the parallel development of teams abroad, who provided security services to Pay TV operators while also hacking the CAS and its Trade Secrets within the smartcard. These teams increasingly engaged in organized crime, drawing serious attention from Interpol and Europol since 2010.

As said above, with the development of OTT and the shift of audiovisual piracy towards illegal streaming, hacking Trade Secrets in CAS is less common in the CAS industry. It would be too expensive for hackers to reverse engineer the Trade Secrets and value it by selling pirate smartcards. However, the practices resume for other businesses such as or in the connected cars’, watermarking[1], or 3D printing still relying on the use of similar Trade Secrets.
Inheriting its 20+ years of experience fighting hackers, the Company had ultimately developed a Secure Manufacturing Platform (SMP) providing for security of digital assets and their traceability across the supply chain. This SMP is a sort of CAS, securing the manufacturing, integrated within the printing machine, whether the printing machine is on site or cloud based and permitting full traceability of the various operations performed on it.

Internal Policies and Relationships

2. **What does your Company consider when deciding to protect confidential information with trade secrets?**

INTERNAL AND EXTERNAL TRADE SECRET POLICY

The Company had (and still has) internal Trade Secrets policies covering all the phases, from their design to their safekeeping.

Physical access to the working areas dedicated to designing proprietary algorithms using therefore source code, computing was highly restricted. Visitors, partners, or suppliers would never access these places. In general, all the Trade Secrets were kept in safes onsite on various devices and at various sites of the Company and/ or for certain of them at the bank. Of course, the design of Trade Secrets was carried out on external networks, meaning not the networks currently used within the Company and the access to which is restraint to certain key employees.

Source- codes mainly related to decoders as well as smartcards algorithms were systematically deposited with a special agency in France (APP). The French APP (Agence pour la Protection des Programmes) is a European organism in charge of protecting software, mobile Apps, data bases, web sites and strategic data. At APP, companies can file for the protection of their digital creations on a secured platform and define within the framework of an escrow contract the terms and conditions pertaining to access and/or the release by APP.

[1] Digital watermarking is used to trace copyright infringement. In essence, it is a security measure based on Trade Secrets meant to discourage and deter piracy while determining the validity and ownership of digital media.

The parts of the Trade Secrets needing to be supplied to the Pay Tv operators were protected in highly secured PCs, serving as safe to secure for instance the cryptographic processes run to generate, protect and manage the keys used for encrypting and decrypting data and for creating digital signatures and certificates.

Same security constraints applied of course to the manufacturers of smartcards having to follow the security norms and standard of the bank industry for the payment cards if not exceeding them. The number of such manufacturers was rather limited. Audits were of course carried out by the Company prior to any signature of contracts with such manufacturers.

THE INTERNAL AND EXTERNAL LEGAL/ CONTRACTUAL ENVIRONMENT

FOCUS ON NON-DISCLOSURE AGREEMENTS - NON-COMPLETE AGREEMENTS- NON SOLLICITATION AGREEMENTS - Roles and difficulties

Signing NDAs when meeting with a new business partner or prospect business partner is a must in this industry and has always been standard. The Company used to raise hundreds of non-disclosure agreements (NDAs) per year. Those NDAs were valid for a limited time period (for example, 1-2 years). Limiting the duration of the NDAs to one or two years gave us the possibility to internally review all NDAs once a year and possibly to get back the confidential information from the (prospect) business partner.

It has recently become more difficult with “younger” generations of potential business partners in the industry to get them sign NDAs because given the highly competitive environment, they would very often see the signature of NDAs as considerably slowing down discussions and interest for the technology. This means that you constantly need to “educate” internally to remind what is to be treated as ”confidential information”. Confidential information of course encompasses the Trade Secrets but also information such as prices, products and business strategy, the way of implementing various technologies, business partners. In addition, information that needed to be shared was marked as proprietary and confidential.

Before issuing any leaflet on the CAS technology, the Communication team used to work with the Legal and IP team (two patent engineers part of my team), checking the general description of the technology. I further used to read the commercial proposals issued by the commercial team prior to they sent them to the customer to ensure that it was not disclosing any confidential information.

Beyond NDAs, reinforced and detailed confidentiality clauses were included in all contractual agreements such as licensing agreements, contracts for the supply of products, purchase contracts, service contracts, partnering contracts etc. (together the Contracts).

All contractual clauses provided prohibited reverse engineering, meaning all the tasks associated with figuring out how to create the software as well decompiling (using tools for reverse engineering) and disassembling (using tools providing for restoring the text of a program for the purpose of figuring out how it operates).

The Contracts generally contained clauses dedicated to safeguard the trade secret. It was, For instance, the customers licensed under the CAS technology were requested to store the encryption keys in saves in highly secured offices with restrictive access, Further, the Company requested to expressly nominate those employees authorized to manipulate these encryption keys.

Constant monitoring of the respect of Contracts ‘obligations in terms of security was carried out, these requirements were gathered in documents such as product specifications, requirement specifications supplied upon signature of the Contract. On top of these provisions

as encryption is a very sensitive matter regulated by international laws and treaties such as the Wassenaar agreement, we had specific provisions asking our customer to guarantee that they had all the necessary authorizations and/or declarations delivered by dedicated authorities for the use or import of the Trade Secrets containing encryption means. Compliance with such legislations was as a condition precedent to the related Contracts as well as the obligation to constantly track the location of such Trade Secrets. Very often audits were carried out on their environments, and it has been the case that the Company declined business with Pay TV operators in countries considered as too “sensitive” to avoid that the CAS technology and related Trade Secrets be put at risk and used for purposes other than Pay TV.

All employment agreements systematically contained non-compete and non-solicitation clauses. Given the applicable legislation (France in this particular case), these types of clauses needed to be limited in time and scope. We used to limit them to 6 months and of course you need to give a financial compensation for this. All these clauses represent a” sine qua non” a minima protection, it does not mean that it protects you 100% but at least it allows you to introduce if needed a legal claim in case of breach.

Having said this, beyond the theory, you had the practice, and in this very small and highly competitive CAS world, it had become common practice for certain of our competitors to hire their competitor’s key employees. We could stop the hiring process several times. As in each company especially when there are many Trade Secrets, the most effective way remains for the Company to have adequate internal effective policies and valid retention programs likely to retain the employees and not to solely rely on these types of clauses.

Another point of attention was with the sub-contractors. The more you use the services of sub-contractors, the more you have risks for your sensitive information and for your Trade Secrets. More and more, companies are confronted to severe employment policies making that they have to recourse to sub-contracting to perform certain developments as they cannot hire employees. The same sub-contractors are working for all actors in this small segment of industry, hence the risk for confidentiality despite all the clauses of the Contracts. For highly sensitive information, we used to double the Contracts with individual confidentiality undertakings signed by the personal of the sub-contractors so that they feel personally concerned and do not think that this is the sole concern of their employers. This is another way of creating individual awareness around confidentiality.

CONSTANT INTERNAL TRAINING AND AWARENESS

As a company with a business vastly relying on secrecy, it is essential to constantly train and maintain internal awareness on trade secret protection and confidentiality measures. For example, we t organized systematically newcomers together with yearly sessions for the whole company. In addition to trainings on confidentiality, we had regular training sessions for contracts in general, with a first focus on NDAs.

INCREASING ROLE OF IT - THE IT CHARTER AND GOOD PRACTISES

IT charters have been fundamentally revisited within the Company’s mother company recently. By reminding good practices in terms of use of the e-mail system and in general of the internal networks and communication tools, this is another way of enforcing secrecy and reminding good practices in terms of handling confidential and sensitive information.

External Policies and Relationships

3. **How do you manage specific risks to the confidentiality of your information arising from external relationships? How do you share your trade secrets**

NDAs first

As said above, signing an NDA is a very first step for your protection. It should clearly list the Confidential Information exchanged. More and more NDAs define penalties to be paid in case of breach; in our context, it would have been extremely difficult to put a figure, as all the business was at stake. In such a case, you can put several million euros as a penalty, but it would still be worth to breach the NDA and get your business and its trade secrets! If needed, it is better to let the courts decide of the amount.

The Applicable law

This is always the friction point as nobody wants to have its confidential information be regulated by foreign courts. Here again, in the course of my career, I have observed various trends. Recently, instead of electing a joint so called" neutral law", we could institute a "dual law and courts" approach that worked quite well. Our Confidential Information would be regulated by French law and courts and vice- versa for our contractual partner. This was considered as perfectly OK at the stage of the NDA to facilitate the exchanges. You have to be open to all these variants, especially as an SME and play with these various approaches, depending on the degree of sensibility of the information exchanged.

Highly sensitive information

In certain cases, for instance in case of an assessment of the CAS as described above, NDA was clearly not sufficient. You need to establish a true protocol, to define in advance which part of the Trade Secrets can be displayed, to only one person, very often the director heading security on- site, at the Company's location and in its presence, with no right to take notes or pictures, and for a limited defined period of time. The reports to be derived from the assessment should be kept in safes. Same physical constraints and restrictions were applying in case of disclosure of certain parts of the technology in the context of due diligences, meaning in case of potential sale of the Company. These due diligence processes were real dangers in terms of confidentiality but not only. It was not of a surprise when one of our competitors having carried out a due diligence process came back to our offices several months after with a notary to carry out a seizure alleging that the Company was counterfeiting their technology. It happened to the Company as well as to other competitors, that was part of the means of trying to undermine the value of a company by opening its trade secrets so that the purchase price could be less.

Enforcement Measures of Trade Secrets – Best practices for monitoring potential misappropriation and resolving disputes

4. **Do you implement any specific measures to monitor potential trade secret misappropriation**?

The experience we had showed that beyond the measures we outlined above in terms of confidentiality, the real way of monitoring potential misappropriation of the technology was to conduct intelligence.

Hacking of smartcards Trade Secrets had become a general practice. One of our competitors had been sued by Canal Plus early 2000, for the sum of one billion USD, as Canal Plus alleged that the software engineers of that competitor cracked the decryption technology contained in the smartcards. Several similar cases followed.

Conducting intelligence had a cost. In the early days, it was certainly" easier" to get information as all these hacking networks and actors were quite visible and open. This is certainly less the case now as you have to conduct such intelligence in the dark web and within private forums, which makes it even more difficult. Conducting intelligence is valuable and sends signals that you are surveying the market and know what is happening. One of the weaknesses of many hackers was to be identified.

5. **How do you resolve potential disputes regarding trade secret misappropriation?**

As said above, we had several courses of action, via intelligence, via direct approach of the pirates and also via the courts, both in France and abroad. Success in these court cases was not given, for instance in Algeria, the Company sued a fraudulent decoder manufacturer but because the decoder manufacturer was key to the region in terms of employment, the local courts were quite reluctant in judging the case and dismissed the charges.

In France the Company could be more successful but sometimes the judicial process took twenty years after introduction of the case and in some circumstances, the businesses of the pirates were no more existing since long given the shift of piracy.
In all these cases, the difficult parts were (i) the basis upon which to build your case, (ii) the supply of evidence and (iii) the technicity of the matter requesting solid technical knowledge from the judges and police officers.

Unlike counterfeit, for which you have a very solid legislation permitting large scale actions such as major seizures, cryptographic keys and proprietary algorithms, these are not considered as intellectual property as they are randomly generated. Therefore, you cannot rely on counterfeiting legislation. When decrypting these cryptographic keys, hackers can understand how the codes execute and they can from there build a sort of "equivalent" of the smartcard, meaning they can" emulate" the principal functions of the smartcard, the same happened to the decoders integrating the smartcard functions. It is very difficult to catch these situations legally.

One of our competitors tried to launch an action in the beginning of the years 2000 as their smartcard had been hacked. The court requested them to disclose the original proprietary algorithm subject of the hack to check their allegation and of course they refused to do so, meaning that they had to drop the case.

Most of the actions have been based on either unfair competition or intrusion into an automated data processing system and evidence is not always easy to submit to the court. In addition, judges need a good understanding and interest in the technology.

The importance of anti-piracy associations

This is also the time when the CAS suppliers and related Pay TV operators gathered into associations, one of them in Europe being the AAPA (Alliance against audiovisual piracy association, previously called AEPOC) which I co-created twenty years ago. One of the tasks of these associations was to brief the police, the courts and prosecutors, bodies like Interpol and Europol, entities like the EU IPO of Alicante on all this audiovisual piracy and related technical implications. We introduced them to the CAS technologies and even prepared for them online courses in many languages so that they could in turn train their people internally.

CONCLUSION

Businesses based on Trade Secrets are more and more at risk and you need to constantly challenge (for instance via penetration testing), renew such Trade Secrets, to constantly survey the market to be able to detect any violation. Due to the money behind protected programs like prime video or sport, hackers will find means to access such programs at their benefit, either via illicit smartcards and decoders in the early days of piracy and now in the days of illegal streaming via illegal websites, dark- web, private forums, social networks or illicit Apps. Hackers rely on organized networks, highly involved in cyber and organized crime. This is a major issue, which has totally undermined the business of the Pay TV operators and now of the platforms owners. Further, it has endangered the subscribers as well as it now threatens and steels their data Constant education and awareness, together with intelligence and monitoring should be made within the companies running trade secrets. Public and private bodies should understand them to adapt legislation.