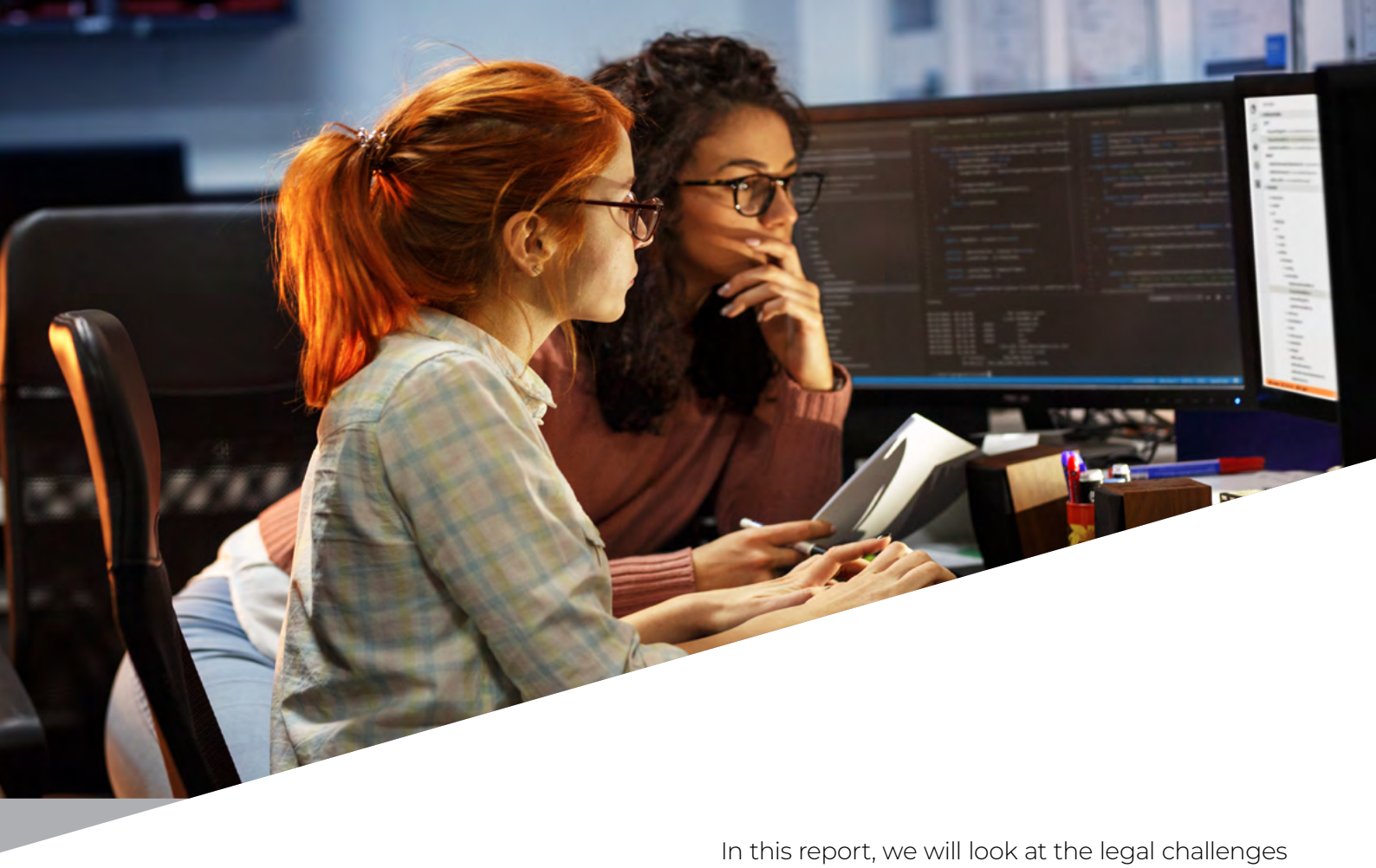
GJE Intellectual Property

Cybersecurity: Strategy for Patents

Contents



Introduction

The growing number of high-profile cybersecurity incidents in recent years, ranging from data breaches to crippling ransomware attacks, has highlighted the critical importance of cybersecurity to modern life. No company or organisation is immune to such threats and most people are by now familiar with almost routine phishing attacks and other forms of cyber-threats. The move towards home working, triggered by the COVID-19 pandemic, has further increased our reliance on technology and, for some, exposed new vulnerabilities. Cybersecurity (or cyber security, depending on your preference) is something we must all think about and the importance of the sector will only continue to grow for the foreseeable future. Accordingly, double-digit growth is predicted, with the cybersecurity market forecast to reach a value of around $193B (USD) in 2028.

Although dominated by US companies, there is healthy competition from other parts of the world with some notable UK giants like Sophos and UK unicorn Darktrace. Such companies derive their billion-pound valuations from their IP but how much of this is protectable through the patent system?

In this report, we will look at the legal challenges faced in this area (focusing specifically on Europe and the UK), review the filing trends and highlight some of the key considerations if patent protection is desired in the UK or Europe more generally.

Cybersecurity is a broad term encapsulating protection against a multitude of different threat types. We have broken it down into the following areas:

- Computer Security
- Privacy
- Fraud

Before delving into these technology areas we will provide some general background on the approach adopted by the UK Intellectual Property Office (UKIPO) and the European Patent Office (EPO) towards assessing the patentability of computer-implemented inventions.

UK Approach

Section 1(2) of the Patents Act 1977 lists examples of subject matter is that excluded from patentability, including anything which consists of a program for a computer 'as such'. The process for determining whether a claim falls within an excluded category is laid out in case law as follows:

i. properly construe the claim;

ii. identify the actual contribution;

iii. ask if this falls solely within an exclusion;

iv. check if the actual contribution is technical.

Step ii., which is essentially where the 'as such' question gets decided, has been equated to asking 'what the inventor really added to human knowledge'.

Later decisions provided what is known as the 'AT&T signposts', which are considered to be helpful when assessing whether a computer program makes a relevant technical contribution. These are:

(i) whether the claimed technical effect has a technical effect on a process which is carried on outside the computer;

(ii) whether the claimed technical effect operates at the level of the architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run;

(iii) whether the claimed technical effect results in the computer being made to operate in a new way;

(iv) whether the program makes the computer a better computer in the sense of running more efficiently and effectively as a computer;

(v) whether the perceived problem is overcome by the claimed invention as opposed to merely being circumvented.

Applicants (or their representatives) arguing the patentability of a computer-implemented invention often need to structure their arguments within the above tests, highlighting how the invention makes a technical contribution and therefore goes beyond a mere computer program 'as such'.

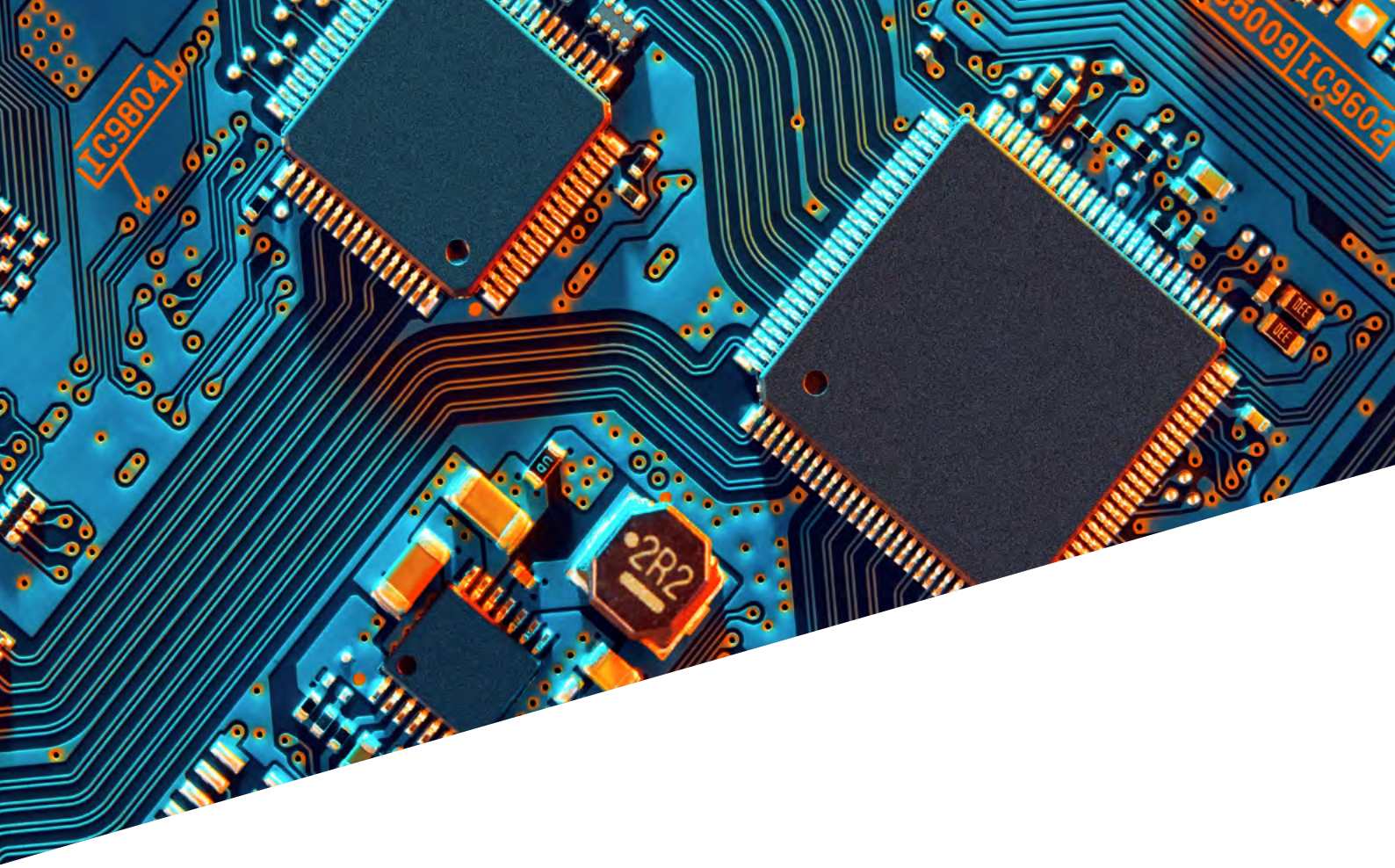
EPO Approach

In Europe, the question of whether a computer-implemented innovation is patentable requires an assessment of whether the innovation produces a 'further technical effect' that goes beyond the normal technical effects of operating a computer (e.g. transistor switching). Unlike in the UK, we are directed to focus specifically on the novel features of the claim with respect to the closest prior art and then ask whether these novel features achieve a technical effect. If a technical effect is not produced, then the innovation will be found to be unpatentable for lacking an inventive step over a general-purpose computer. However, there is no precise definition of the term 'technical'. This is by design to take account of the ever-changing nature of technological developments.

For computer-implemented processes we normally look for an improvement in the operation of a device or a particular process. In the case of computer-implemented inventions we are often looking to frame the invention as providing an efficiency improvement, increased security or enhanced usability - to name but a few examples.

Of most relevance to cybersecurity is clearly 'increased security'. A computer-implemented invention which, when contrasted against the closest prior art, improves the security of the computing system, should in principle be deemed as technical and therefore relate to patentable subject matter.

For both the UKIPO and EPO, assuming that the hurdle of showing that the invention relates to patentable subject matter can be crossed, applicants will next need to argue why the novel aspects of the claim constitute a non-obvious development over the prior art as a whole. This is assessed in the normal manner which applies across all fields of technology.



Computer Security

This is the technology area most traditionally associated with cybersecurity. We have used the term 'computer security' to encompass protection against cyber-threats directed at compromising the actual operation of a computing system, such as anti-virus software, network-intrusion detection software, etc. These threats may occur within different types of computing systems including a computer, computer network, virtual machine or cloud-computing environment. Inventions in this area are generally directed at detecting threats, preventing the system from being infected and/or curing a system that has been infected.

When assessing the patentability of such inventions the UKIPO has adopted the approach that the contribution provided by the invention needs to go beyond merely identifying the presence of a security threat. Unless a further step of remediating the threat is claimed and therefore forms part of the contribution, the computer does not actually run any more effectively and so the fourth AT&T signpost is not met. The remediating step can be broadly expressed within the claim, however in the absence of claiming this step, the invention will generally be treated as a non-patentable computer program 'as such'

This is supported by the vast majority of cases we have reviewed in this area. In the case of GB1610609.8 (Sophos Limited) the examiner wrote:

> *As discussed above, merely examining objects does not provide an improved computer. If the objects are compromised this might identify them but it does nothing to remedy that compromise. Therefore it is maintained that the fourth signpost is not met...it is agreed that performing remediation could potentially give rise to a technical effect. However as presently claimed no remediation is performed. It is therefore maintained that claim 1 is considered to be excluded from patentability as it relates to a computer program, as such.*

Similarly, comments were provided by the examiner in the assessment of GB1900639.4 (IBM Corp.) Likewise, in GB2011381.7 (Sophos Limited) the examiner addressed each of the AT&T signposts as follows:

> *The alleged inventions relate entirely to data processing carried on within the computer. They do not involve an effect on a process outside the computer. The first signpost is not met.*
>
> *The alleged inventions operate at the application level of the computer and operate on specific types of data (i.e. malware samples). They do not involve an effect at a higher level of generality within the computer. The second signpost is not met.*
>
> *The alleged inventions involve operating the claimed programs, but this does not result in the computer being made to operate in a new way. Even if the programs are new, the way the computer operates in the sense of how it executes programs on a fundamental level is not changed. The third signpost is not met.*
>
> *The alleged inventions may provide improved ways of generating an anti-malware system, but they do not do so by making the computer on which the programs are run operate more efficiently or effectively as a computer. The fourth signpost is not met.*
>
> *The perceived problem is that "...There remains a need for techniques to enhance training of machine learning systems in order to improve the detection of new, previously unseen malware threats". This problem is not technical in nature as it relates to the relevance of training sets to the scenario in which a machine learning model is deployed. As the problem is not technical in nature the fifth signpost does not apply.*
>
> *Claims 1 and 20 are therefore considered to be excluded from patentability as they each relate to a computer program as such.*
>
> *However,* ***dependent claim 19 refers to detecting malware and initiating a remediation of the detected malware. Claim 19 therefore appears to involve a technical contribution.*** *It is considered that including such a remediation step in the independent claims could be one way to address the above objection.*

Detecting a threat is generally not enough. UK examiners often insist on a remediation step being claimed to avoid being excluded from patentability

Applicants may disagree with the restrictive manner in which some of these signposts have been applied, however the UKIPO appears to be developing precedence in this area which, in the absence of any decisions from the UK courts on this issue, will determine how applications will be examined.

Since claims will need to be limited to the remediation step itself, which may be performed by a customer rather than a competitor, it is important to include a claim to a computer-readable medium in the UK at least in addition to a standard computer-implemented method claim. This will cover computer code that is configured to perform remediation, with such code being produced and shipped by competitors and hence making direct infringement of a claim more likely.

The situation at the EPO is slightly different. European patent examiners do not need to consider the "contribution" provided by the invention as a whole, nor the AT&T signposts. Improving the security of a computing system is accepted as being technical, regardless of whether the claim includes a specific step of remediating any threats that are detected. The examiner needs only to look at the novel part(s) of the claim, consider the effect, ask whether it is technical and then move on to considering inventive step. We have therefore seen a greater number of applications granted in this area with claim scopes not including remediation. For example, in the case of EP3588350 (AO Kaspersky Lab), claim 1 ends with a step of "pronouncing a decision as to harmfulness of safety of the executable file based on the results of the asynchronous search." Other examples are provided by EP3477522, EP3361407 and EP3246842 (each to AO Kaspersky Lab) in which claim 1 concludes with a step of performing an antivirus scan or notifying the user of a threat.

At the EPO improving the security is accepted as being technical, regardless of whether the claim includes a step of remediating any threats

In Europe, we have found it is only in the instances in which the patent specification has been drafted so as to suggest that taking remedial action forms an essential part of the invention, that the examiner insists it forms part of the independent claims. This issue arises under the assessment of clarity, rather than patentable subject matter, and the European principle that the independent claim(s) must include all "essential features" necessary for achieving a technical effect underlying the solution of the technical problem with which the application is concerned (the problem usually being derived from the description). This was the case in EP12852500.3 (McAfee, LLC) where the examiner noted:

> It *is clear from the description that the problem solved by the present application is to prevent malicious attacks. However, the present independent claims only solve the problem of determining a malicious action. Therefore, in order to solve the stated problem, the features indicating what steps (e.g. steps 955 and 970) to perform when it is a malicious action or not are essential to the definition of the invention.*
>
> *Since the independent claims do not contain these features they do not meet the requirement following from Article 84 EPC, taken in combination with Rule 43(1) and (3) EPC, that any independent claim must contain all the technical features essential to the definition of the invention.*

Applicants can typically ensure they do not fall into the trap of being forced to unnecessarily limit the scope of the independent claims for a European application to include a remedial step at the stage of drafting the application. In particular, the discussion of the problem solved by the invention and the benefits conferred should generally avoid suggesting that a step of remedying or preventing malicious attacks is fundamental to the invention.

On the basis of this information, applicants might conclude that the EPO provides a more favourable assessment of computer security patent applications when compared with the UKIPO. Whilst this appears to be true of applications not claiming a remedial step of taking action against a detected threat, if the hurdle of patentability can be overcome, it is generally accepted that the UKIPO employs a slightly lower bar when assessing inventive step than the EPO. Accordingly, applicants having inventions inherently claiming a remedial step may have a better probability of obtaining a broader claim scope when prosecuting their application before the UKIPO in contrast to the EPO. This underlines the importance of obtaining professional advice at an early stage in the procedure, ideally prior to filing any applications, in order to determine the best prosecution strategy for any given invention.

Privacy

Though there is substantial overlap between privacy and computer security, digital privacy can be very generally described as giving an individual control over how their information is used. To illustrate this further digital privacy can be broken down into the following categories: information privacy, communication privacy, and individual privacy — though these are not mutually exclusive. For example, information privacy describes how an individual should have the freedom to determine how their data is collected or used; laws such as the EU's GDPR and the UK's Data Protection Act enforce this. Communication privacy concerns the secure exchange of information between parties using technologies such as encryption, meaning that a transmitted communication will only be accessible to the sender's originally intended recipient. Lastly, individual privacy refers to an individual's right to exist freely on the internet so they can choose what information they are and (critically) are not exposed to. Tools such as ad blockers and spam filters would fall into this category.

The UKIPO and EPO do not explicitly distinguish between the above categories and instead assess an application on its own merits. However, it is worth noting we expect inventions relating to communication privacy to generally be considered as more technical than those relating to information/individual privacy due to the focus largely being on the security of a device itself, irrespective of how it is used and the intentions of the user.

At this time the UKIPO has not set any clear guidelines to follow for privacy as they have with computer security discussed above. Examiners still use the AT&T signposts to help consider whether a privacy focussed computer program makes a relevant technical contribution. However, the topic of privacy has appeared in several hearings at the UKIPO and these can examined to help further guide drafting and prosecution of privacy related inventions.

In the 2019 decision O/611/19 for GB1715687.8 (Google LLC), the hearing officer wrote:

> *In my view, the issue of security and privacy for users when using computing devices is a technical problem which has an effect outside of the computer/computer system.*

Inventions to communication privacy are likely to be considered as more technical than those to information or individual privacy due to the focus on the security of a device itself, irrespective of how it is used and the user's intentions

This is a clear positive linking of a user's digital privacy to the first AT&T signpost. The invention was determined to have an inventive step and the application went on to grant, in spite of none of the other signposts being met.

A 2020 hearing went on to clarify the teachings of the Google decision. In the hearing O/402/20 for GB1708043.3 (F-Secure Corporation) the applicant sought to use the Google decision to overcome an excluded subject matter objection. While the applicant was ultimately unsuccessful, the comments from the hearing officer did expand upon those made in Google:

> *There is no doubt that the area of privacy and security when using computing devices is one in which technical contributions may be made, but I consider it would be wrong to interpret the hearing officer in Google to have said that any invention that relates to privacy and security will necessarily avoid the exclusions of section 1(2). The above quotation cannot be stripped of its context, and that context is significantly different to this application…*

> *The question…to answer here is whether the effect of preventing user data from the client device from being passed to the tracking service constitutes a technical effect. There can be no doubt that it enables the user to keep certain information from the tracking service, but is that technical? If maintaining user privacy is a technical problem then I might possibly accept that preventing the user's data from being passed from the client to the tracking service could be a technical effect.* ***But in this instance, at least, maintaining user privacy is not a technical problem.*** *The problem, such as it is, only exists because some internet users do not want tracking services to be able to gather data related to them, but they still want a smooth online experience. Other users may be perfectly content to trade the tracking of their online behaviour for a smooth online experience, whilst still others may be indifferent, and for these users and their devices there is no problem at all. The invention may satisfy the desires of the first group of users, but this does not mean that there is a technical effect on their client devices. It does not solve a technical problem on the client device, or on the proxy server.*

As many will have come to expect, the situation at the EPO is similar to the UK but it is worth taking note of differences and definitive decisions. Though there is not currently a general rule applied to digital privacy related inventions, the EPO Board of Appeal has provided several recent decisions that address specific points related to privacy.

A key decision was T 1248/12 (Crossix Solutions LLC), issued in 2019, which related which related to data privacy in a database system. In making their decision, the Board determined that:

> *De-identifying data, by removing individually identifiable information, and by aggregating data from a plurality of sources, is not technical.*
>
> ***Protect[ing] data privacy … is not a technical problem.*** *The problem of data privacy is not synonymous with data security. Data privacy concerns what information to share and not to share (and making sure that only the information that is to be shared is shared), whereas data security is about how to prevent unauthorised access to information.*

The hearing officer did not dispute that security and privacy for users of computing devices can be technical issues, but emphasised that this does not mean that any related invention is technical. The hearing officer argued that the Google application was not excluded because it required the retrieval and processing of images from the "real-world" in order to identify a user also in the "real-world" and so met the first signpost in this way. However, the hearing officer was not convinced the user data of the F-Secure application (such as credit card data and web browsing behaviour) provided the same real-world effect.

Although a rule for deciding exactly when privacy is considered a technical issue at the UKIPO has not been set, it is certainly apparent that context is key and the more that an invention can be linked to the physical world the better.

It is best to present a privacy invention as providing digital or computer security

T 1150/13 (Tra Inc.) of 2020 reinforces these positions, where the Board again took the view that de-identifying personally identifiable information (PII) is not technical in and of itself, saying that:

> *the protection of privacy, by replacing PII (an address) with non-PII (a key) is not technical. It is an administrative scheme or a mental act.*

The EPO makes a clear distinction between data privacy and data security, with the latter providing a technical problem while the former is considered an administrative scheme. Although preventing unauthorised access to information could be interpreted as falling within a broader meaning of "making sure that only the information that is to be shared is shared", the EPO has made a clear distinction between the two. For the EPO, it is typically key to frame a data privacy application from the perspective of preventing access to the data.

Though this approach may appear relatively restrictive at first glance, we have found a large number of privacy related applications granted at the EPO. Some methods of increasing privacy have also been directly acknowledged as technical (though it is still best to describe these as security improvements). For example, in the 2020 decision T 2327/17 (Robert Bosch GmbH), the Board of Appeal determined increasing "the cryptographic security of an audio data stream" was a technical problem.

In summary, it is best to present a privacy invention as providing digital or computer security when filing an application at either the UKIPO or EPO. The above considerations regarding claiming a remediating step have particular relevance for applications before the UKIPO.

Fraud Detection

Fraud is unfortunately likely well known to all of us as it most typically arises in the context of electronic payment systems. Fraud takes many forms — card cloning, skimming, over the shoulder attacks, replay attacks, phishing and others. What is common about all of these techniques is that the attacker attempts to authenticate themselves as a genuine user (e.g. a cardholder) and to interact with a payment system to somehow trick the system into performing an action that benefits the attacker — typically, to transfer money or assets to the control of the attacker.

While there is clearly a computer security element to fraud detection, this falls more into the preventative category. There is also the act of fraud prevention itself — i.e. detecting an attempt at fraud, perhaps in real time, and stopping it. It can be more difficult to frame inventions directed to fraud detection and prevention as improving computer security, and so in such cases it is necessary to understand whether fraud prevention *per se* is patentable.

EPO case law divides fraud detection and prevention into two very distinct categories — technical fraud protection that is based on understanding of a technical element of a system vs. non-technical fraud protection that is based on business or administrative rules in a payment system or equivalent. The following discussion examines some EPO Board of Appeal decisions in these two categories.

As can be seen from the cases discussed on the following pages, fraud detection and prevention can be considered both technical and non-technical at the EPO depending on context. In the case of a technical machine like an ATM, features of a fraud detection mechanism that rely on an understanding of how the machine operates are solely within the competence of the technically skilled person. This will lead to a patentable invention, assuming of course that the other criteria for patentability are met. On the other hand, if no understanding of a technical machine is required to arrive at the fraud prevention scheme, the EPO is unlikely to find it to be patentable. Taking one of the highlighted examples, the choice to calculate a probability of liveness does not require any understanding of how the sensor(s) used to gather data to enable this probability to be calculated work. This choice can therefore be made by a non-technical person, in contrast to the situation with the ATM in T 1901/08 (NCR International., Inc.).

It therefore seems that a highly pertinent question to ask when considering filing a patent application to a fraud prevention technique at the EPO is whether the technique required knowledge of a technical entity to invent. If yes, patentability is more likely than in the case where the technique involves non-technical considerations.

Examples of EPO Decisions on Fraud Prevention

T 1386/14 (Eyelock LLC)

The invention at hand in this case related to use of biometric information to authenticate financial transactions. A key aspect of the claimed authentication process was the calculation of a 'probability of liveness', this being a probability of biometric information submitted as part of the authentication process as having being obtained from a living person rather than an inanimate object.

The invention rested on the choice of the 'liveness' parameter for use in the authentication process, with the idea being that attempts to fraudulently authenticate using inanimate copies of biometric information (e.g. images of fingerprints or the use of iris scans) are prevented.

The EPO Board of Appeal found that use of the 'probability of liveness' in the decision as to whether to authenticate the requestor was a non-technical choice, commenting that "the choice of "liveness" as criterion is a non-technical decision as to what sort of identification is acceptable". The Board also drew a distinction between choosing the liveness parameter and designing a sensor to measure data indicative of this parameter, with the inference that the latter would have produced a technical feature capable in principle of supporting an inventive step. The result was that the application was refused.

This decision neatly highlights a key element of the way in which the EPO approaches inventions relating to fraud detection and prevention. As shown in this case, it does not help if aspects of the fraud detection process that derive from business or administrative considerations are implemented using a computer, biometric sensor or other such clearly technical means. This is because EPO examiners do not need to find an example of technical means configured to carry out non-technical steps. Instead, the non-technical steps are added to a list of requirements that is to be given to the notional skilled person tasking with designing a technical system that meets said requirements.

Mapping this to the facts of T 1386/14, the concept of including a liveness parameter in an authentication process was therefore automatically deemed to be unable to support an inventive step irrespective of the content of the prior art. All that is needed to show this to be obvious is therefore any disclosure of a technical means suitable for measuring a liveness parameter even if the disclosure does not say that liveness is being measured. This is the key take home from this decision.

T 0977/17 (Otto Group Solution Provider (OSP) GmbH)

This case concerned a payment 'certificate' (receipt) tracking system that keeps track of paper and electronic receipts generated by financial transactions. The receipts are stored electronically and published online to enable data to be extracted from the stored receipts, e.g. to enable research into consumer purchasing habits. The majority of the decision is out of the scope of this discussion, but it is worth noting the Board's response to a suggestion by the appellant that a technical effect of the system was to prevent attempts at fraud using fake receipts since the fake receipts could be detected using the data published online. On this the Board commented:

> *However, business fairness, accuracy of business data and the users' trust in the system are non-technical parameters and improving them by publishing payment certificates within resale offers is still a purely business decision not involving any technical considerations.*

The most interesting comment here is that "the users' trust in the system [is a] non-technical parameter". It is often the case that one can rely on 'improved user experience' as a technical effect realised by a computer program, but it seems that this is not so when the improvement relates to the trustworthiness of a system. As a result, the appellant was unable to convince the Board that an inventive step was present such that the application was refused.

T 1901/08 (NCR International., Inc.)

This case related to detection of a 'traditional' type of fraud, namely fraud at an ATM. The invention provided a card reader jamming detector and a set of 'software agents' that were each assigned to a particular component of the ATM. One such software agent was assigned to the jamming detector. A 'higher level' software agent managed the set of software agents and was configured to raise an alert indicative of potential fraud taking place based on the jamming detector detecting a card jam and a particular state of another of the set of software agents, e.g. a PIN entry monitoring software agent or a cash dispenser monitoring software agent. The invention therefore was specifically suited to detecting attempts to commit fraud by tamping with the card reader of an ATM.

The application was initially refused by the EPO Examining Division, with this refusal being overturned on appeal. The Examining Division based a finding of a lack of inventive step on the rationale that the detecting of card reader-based fraud was a non-technical decision taken in response to the detection of significant amounts of card reader-based fraud. In the Examining Division's view that made it appropriate to formulate a requirements specification that set the skilled person the task of making a card reader tampering detection device. Faced with this requirement, the skilled person naturally arrived at the invention without difficulty.

The Board disagreed with this and found that instead technical considerations were involved in the detection of card reader-based fraud. This was because, in the Board's view, detecting card reader-based fraud in this case relied "on a technical understanding of the operation of the terminal and its respective components and, thus, lies within the scope of a technically qualified person working in the field of self-service terminals." The Board therefore overturned the decision of the Examining Division and ordered grant of a patent.

Contrasting the EPO and UK Approaches to Software

A good rule of thumb is that, in general, the lower the level at which the computer invention operates, the more likely the invention is to be patentable at the EPO; however, simply using known hardware components does not make an invention patentable.

A relatively high-level invention may be considered technical if the relatively high-level program is designed based on specific technical considerations relating to the internal function of a computer or to solve a technical problem. In the case of cybersecurity related inventions, it is often possible to argue that the technical problem being solved is improved security of a computer and data stored on it or being transferred between computers.

A computer program may be designed based on specific technical considerations of the internal functioning of the computer on which it is to be executed, if it is adapted to the specific architecture of the computer. Computer programs implementing security measures for protecting boot integrity or countermeasures against power analysis attacks have been provided as examples by the EPO because they rely on a technical understanding of the internal functioning of the computer. Some cybersecurity related inventions, such as antivirus programs, are designed to run on particular operating systems, and so the internal functioning of the computer on which the antivirus software is being run has to be taken into account. Similarly, application-level security programs rely on a technical understanding of the application program, and so these should be patentable in accordance with the EPO's guidelines.

The EPO is usually more friendly towards computer-implemented inventions than the UKIPO

The equivalent requirement at the UKIPO is whether the claimed technical effect operates at the level of the architecture of the computer; that is to say whether the effect is produced irrespective of the data being processed or the applications being run. This can be considered to be more restrictive than the EPO approach. UK examiners often insist that a patentable CII should operate at the lowest level of a computer by making reference to the architecture, or hardware, of the computer. In addition, the UK test is often interpreted as excluding application level programs by requiring the program to be application independent.

Whilst the intention is for the UKIPO approach to be in line with the EPO approach, in practice the two approaches have some subtle but important differences which can prove relevant for cybersecurity inventions. Although there may be some exceptions (for example, where remedial steps are claimed), our experience is that the EPO is usually more friendly towards computer-implemented inventions than the UKIPO. We would therefore generally advise seeking protection for computer programs and software in the UK via a European patent application filed at the EPO instead of filing a UK national application. There are always exceptions, for example as discussed above under the header 'Computer security'. Each case should be assessed on an individual basis to determine the appropriate filing strategy.

A Look at the Statistics

We have conducted a detailed review of patent application filings in the cybersecurity and present the full results in the attached annex. In short, the results agree with our observations above that the UKIPO more often tends to take a more negative appraisal of patent applications in this technology sector compared with the EPO or USPTO. The USPTO and UKIPO generally examine applications faster compared with the EPO, and the applicants filing the highest number of patent applications are generally the US corporates. Greater parity in the examination of such patent applications is desirable to provide UK and European software companies with the adequate incentives to grow their businesses and compete with any US rivals. This may require a reform to European and UK patent law to broaden the patentability of computer-implemented inventions.

> A determinative factor relates to how the invention is communicated within the application

Conclusion

As with all fields of technology, it is useful to evaluate the reasons for seeking patent protection for a particular idea prior to preparing and filing any application. Applicants should be conscious of the risks of publically disclosing valuable trade secrets through the patent prosecution process if the odds of the application progressing to grant are slim. On occasion, relevant business concerns, such as a desire for a pending application to improve odds of receiving investment, may trump patentability concerns, however each case should be assessed on an individual basis.

Some of the specific considerations affecting cybersecurity related inventions are set out above. In summary, these types of inventions are often patentable but a determinative factor relates to how the invention is communicated within the application. Another question to consider, if patent protection in the UK is desired, is whether the invention is more likely to be positively received by the EPO or the UKIPO — which can depend on the invention in question, though generally favours filing at the EPO. The choice of patent office will also likely affect the length of time that the application remains pending, with the UKIPO typically providing a faster examination of these applications at a lower cost.

Getting the right legal advice at an early stage is therefore essential. If you would like to know about how our expertise in cybersecurity can help you then please get in touch. We welcome enquiries via gje@gje.com.

ANNEX – Statistical insights

Identifying actionable insights from filing data in cybersecurity is not straightforward as applicants don't use helpful terms like 'cybersecurity' in their patent applications. Moreover, cybersecurity is a disparate field covering a wide area. For example, cryptography and the prevention of DDoS could both fall under a large umbrella of cybersecurity or information security; lines between which are often blurred. There isn't even consensus on whether cybersecurity is one word or two. There is no one classification code that exists to cover the wide range of concepts that enables simple filtering. For example, H04L61 covers 'Network arrangements, protocols or services for addressing or naming' while H04W covers 'Security arrangements; Authentication; Protecting privacy or anonymity in wireless networks'. The wide range of classification codes used supports the conclusion that there is a wide spread of technology areas relevant to cybersecurity threats.

If we were to show you that the majority of cybersecurity applications originate from the US with a big increase from China in recent years then you likely wouldn't be very surprised. Instead we've tried to focus on a few interesting points of note.

The following table shows comparison of the time to grant and number of 'dead' applications in the cybersecurity sector as defined based on a keyword analysis for applications filed since 2012, and an indicator of the relative popularity of the USPTO, EPO and UKIPO:

Patent office	# of applications	Av. years to grant	% dead applications
USPTO	114,741	2.7	19%
EPO	28,714	5.4	26%
UKIPO	4,650	3.5	44%

The UK's 'compliance period' puts a ceiling on the length of time an application can take to grant, meaning that on average a quicker outcome can be expected from the UKIPO compared with the EPO.

The percentage of dead applications could be interpreted as providing an indicator of the likelihood of being awarded a patent in this field of technology. However the statistics are skewed by other factors. When comparing the above numbers to the corresponding results obtained for the general fields of electricity and physics, the percentages are broadly consistent (see below). The relatively high number of dead UK applications is therefore more likely a consequence of the fact that the UK is a cheap first filing territory and so often applicants will file UK priority applications, which are allowed to lapse in favour of a later UK or EPO follow-up application, rather than the UKIPO refusing a disproportionate number of applications in this area.

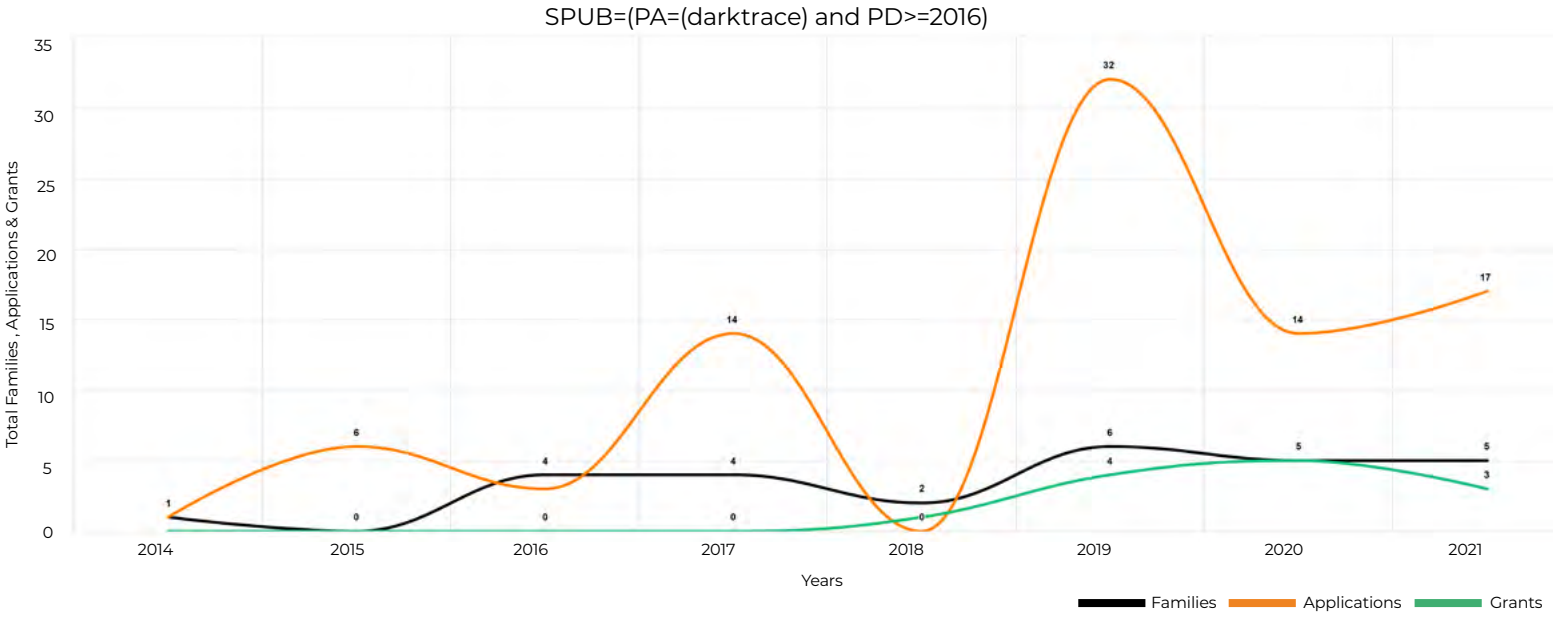
The US clearly remains an attractive jurisdiction in which to seek patent protection for cybersecurity inventions due to the relatively fast examination and lower percentage of dead applications.

In this next set of analysis we have looked at some specific companies in this sector.

In order, the top ten filers of cybersecurity applications in recent years were: IBM, Cisco Tech Inc., Microsoft Technology Licensing LLC, Ericsson Telefon AB L M, Intel Corp., Symantec Corp., Huawei Tech Co. Ltd., Qualcomm Inc., Amazon Tech Inc., and Citrix Systems Inc. This demonstrates that while the smaller players may get all the headlines, the large US corporations still dominate when it comes to patent filings.

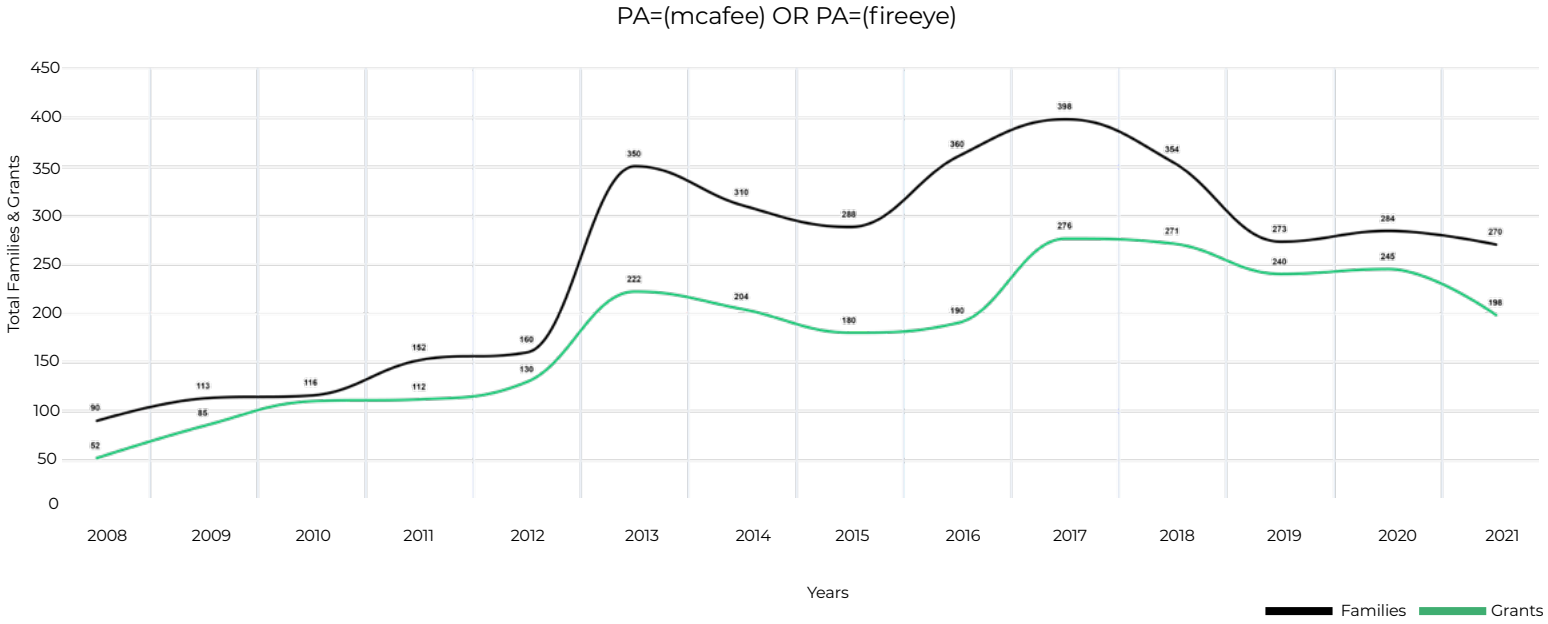
While the big companies will dominate the numbers, filing thousands each, there is still space for a startup. Figure 6 shows the filings for UK-based unicorn Darktrace. As you can see, there is a big uptick in 2019 as the portfolio starts to mature, as they expanded, and (presumably) geared up for IPO. It will be interesting to watch the filings for this innovative company as they continue to expand their R&D efforts following the IPO in 2021.

Patent applications, families & grants (Darktrace)



Other recent commercial activity saw the owners of McAfee taking it public in 2020 and then private again in 2022 following its split from Intel. Fireeye, not long ago the growth story in cybersecurity, was combined with McAfee enterprise to form Trellix, an extended detection and response company. Looking at the filings from these applicants we can see the big growth in filings around ten years ago as the market in cybersecurity really took off for both companies, before a general levelling off in filing activity. Interestingly the US remained a big market for both, but international filings were more considered. It is likely that both companies were more selective with filing, perhaps filing their more important families or being more judicious where prospects of grant were lower.

Patent families & grants (McAfee / Fireeye)



If comparing applications filed in the IPC classifications H04L63, H04W12 or G06F21 (which could be broadly considered to encompass cybersecurity) to the more general H and G IPC classifications (covering electronics and physics) we can see that cybersecurity applications are generally treated consistently.

	IPC = (H04L63 or H04W12 or G06F21)		IPC = (H or G)	
Patent Office	Average years to grant	% dead applications	Average years to grant	% dead applications
USPTO	3.0	21%	3.0	26%
EPO	5.8	32%	4.5	36%
UKIPO	3.5	47%	3.6	57%

For the EPO there is a very similar proportion of dead applications in the cybersecurity field compared with the more general electronics and physics fields. This agrees with the conclusions from our case law review above where we found the EPO has tried to apply a consistent approach to assessing technicality without perhaps treating cybersecurity more negatively. Perhaps the time to grant means the EPO is open to more amendment and argument here which delays the process but leads to consistent pending statistics. Although the percentage of dead applications at the UKIPO is noticeably smaller in the cybersecurity field than the more general electronics and physics category, it is still notably higher than at the USPTO and EPO - suggesting that it is a more difficult to get a granted patent in this sector from the UKIPO. The UKIPO figures are likely significantly skewed by other factors, as discussed above, to appear more pessimistic than the reality, however the general trend is not wholly surprising based on anecdotal experience.

Gill Jennings & Every LLP

The Broadgate Tower
20 Primrose Street
London EC2A 2ES

T +44 (0)20 7655 8500
F +44 (0)20 7655 8501

gje.com