NewStatesman

# Cyber crime and IP theft

## Protecting the digital economy

In partnership with

FAST
Federation Against
Software Theft

CIPA
The Chartered Institute of Patent Attorneys

**Baroness Neville-Rolfe** Anders Jessen **Ed Vaizey** Francis Maude
Alex Hilton **Catriona Hammer** Julian David **Daniel Medlycott**

**Baroness Lucy Neville-Rolfe**
Minister for IP

**Julian David**
Chief executive, techUK

**Doug Davidson**
Director of cyber security services, Capgemini

**Catriona Hammer**
Senior counsel IP, GE Healthcare

**Alex Hilton**
Chief executive, Federation Against Software Theft (Fast)

**Julian Heathcote Hobbins**
General counsel and deputy chairman, Fast

**Anders Jessen**
Head of intellectual property unit, DG Trade, European Commission

**Andrew Joint**
Commercial technology partner, Kemp Little

**Daniel Medlycott**
Detective chief inspector, Pipcu

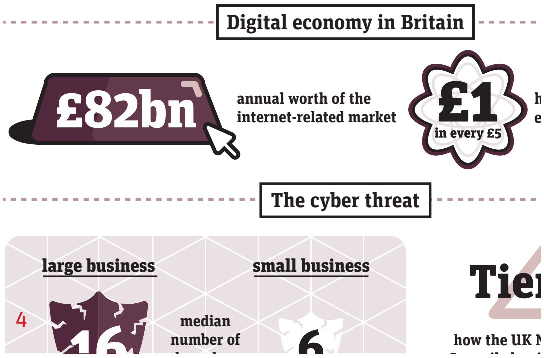
**Jon Bernstein**
Chair

New Statesman
3rd Floor
Farringdon Place
20 Farringdon Road
London EC1M 3HE
Tel 020 7936 6400
Fax 020 7936 6501
info@
newstatesman.co.uk
*Subscription inquiries, reprints and syndication rights*:
Stephen Brasher
sbrasher@
newstatesman.co.uk
0800 731 8496

*Supplement Editor*
Jon Bernstein
*Design and Production*
Leon Parks
*Graphics*
Chris Ong

*Commercial Director*
Peter Coombs
020 3096 2268
*Head of Partnerships*
Eleanor Slinger
020 3096 2275

Round table



Facts & figures

# Crime stoppers

In his excellent BBC series on cyber crime, the journalist and author Ben Hammersley notes how criminals have adapted to new technology. "We call their devious work cyber crime," he says. "Within a decade, we'll just call it crime." Cyber crime is already a catch-all for a number of malicious activities. Some are digitally native, others where information and communications technologies facilitate legacy crimes, passing off counterfeit goods among them.

The editorial thrust of this supplement is the impact that cyber crime, particularly intellectual property theft, is having on the digital economy. One government agency puts the cost at £27bn, a third of which it attributes to IP theft (see Facts & Figures, page four).

The centrepiece of the supplement is a report (see page eight) from a *New Statesman* round-table discussion held last month. Our principal guest, the IP minister Baroness Neville-Rolfe, offered a rallying cry for the knowledge economy – "Britain has to compete on the world stage and we have to use the brains of our people and the strength of our education" – while describing cyber crime as a "real threat to national security" and urging industry, as well as policymakers, to do more to protect IP.

To gain a sense of how all-encompassing cyber crime has become, it is worth noting how many government departments are invested in it from an intellectual as well as a policy perspective. Indeed, Ed Vaizey's role as minister responsible for digital industries traverses the Business and Culture departments. Writing on page 15, Vaizey notes: "As well as protecting assets and IP, good cyber security can boost reputations and provide a competitive selling point."

Meanwhile, his colleague Francis Maude, minister for the Cabinet Office (see page five), insists: "Cyber security cannot just be an issue for the IT department: it's an issue for the boardroom, too." |

This supplement, and other policy reports, can be downloaded from the NS website at newstatesman.com/page/supplements

First published as a supplement to the *New Statesman* of 12-18 December 2014.

Registered as a newspaper in the UK and USA.

The paper in this magazine originates from timber that is sourced from sustainable forests, responsibly managed to strict environmental, social and economic standards. The manufacturing mills have both FSC and PEFC certification and also ISO9001 and ISO14001 accreditation.

COVER: CHRIS ONG

## Digital economy in Britain

**£82bn**

Annual worth of the internet-related market

**£1** in every £5

How much businesses earn from the internet

## The cyber threat

| | Large business | | Small business |
|---|---|---|---|
| Median number of breaches suffered | 16 | | 6 |
| Reported cyber breach | 60% | | 81% |

**Tier one**

How the UK National Security Council classifies cyber attacks

**17%**

of advanced persistent attacks across Europe target the UK

## The price of cyber crime

**£27bn**

Annual cost of cyber crime to British economy

**1/3**

of that figure a result of IP theft

Estimated cost of worst cyber security breaches:

**Large business**

**£600k - £1.2m**

**Small business**

**£65k - £115k**

Sources: Office of Cyber Security; National Security Council; FireEye; AT Kearney/Vodafone; Department for Business, Innovation and Skills Information Security Breaches Survey 2014

GRAPHICS: CHRIS ONG

# How to become a 21st-century cyber superpower

*By Francis Maude*

Companies must manage their own risks. Digital security can't be an issue for the IT department alone: it's an issue for the boardroom, too

When Tim Berners-Lee created the worldwide web 25 years ago, he made it open and free. It was an incredible gift to the world, allowing anyone to use this invention to create new technologies, solutions and opportunities. The digital revolution has brought new choices and speed to the world of business, just as it enables governments to provide public services that are more convenient and responsive to people's needs, at a lower cost to taxpayers. Whatever the threats from the internet, we need an approach to cyber security that helps government, businesses and individuals keep safe online so they can continue to enjoy these remarkable benefits.

Intellectual property theft is a big threat to UK firms – one London-based company had a loss running into the hundreds of millions of pounds as a result. As part of its long-term economic plan, the government wants the UK to be one of the safest places in the world to do business. That's why we've committed to improving our resilience through the UK Cyber Security Strategy, backed by £860m of funding.

Our strategic investment in cyber security has enabled the creation of a National Cyber Crime Unit, within the new National Crime Agency, and a national computer emergency response team, CERT-UK. Together with government departments, GCHQ and other agencies, these bodies are already working to combat cyber criminals, as well as producing guidance and resources for businesses.

But government cannot and should not do this on its own. Companies must manage their own risks. Cyber security cannot just be an issue for the IT department: it's an issue for the boardroom, too. Firms should have tried and tested resilience plans. The good news is that the 2013 Cyber Governance Health Check was completed by almost two-thirds of FTSE-350 companies, suggesting that boards are starting to take the issue more seriously.

Because the cyber threat is anonymous and dispersed, governments and businesses must work together. Last year we launched the Cyber Security Information Sharing Partnership (CiSP). This enables businesses to share intelligence on threats and vulnerabilities as they occur, helping to build a more complete picture of the cyber threats we face. This intelligence has already helped organisations respond to recent threats such as Shellshock, GameOver Zeus and Heartbleed. By the end of October, 683 companies had joined the partnership and it continues to grow.

> UK cyber businesses employ 40,000 people and are worth £6bn

The UK is actively engaged with developments in Europe, particularly the negotiation of the Network and Information Security Directive. We need strong cyber security among all our neighbours. This directive can help, but it should not come at the cost of onerous regulation on business and we will continue to influence the negotiations. After all, the reason our partnership works so well is that it's business-led, which creates trust and means companies are willing to share information in confidence.

We should also recognise that cyber is a business of the future in its own right, creating opportunities for jobs and growth. It's one where Britain has significant strengths. It already employs some 40,000 people and is worth £6bn in the UK. We want to see it grow further. Government and business have teamed up to create the Cyber Growth Partnership, which represents a cross-section of some of Britain's most innovative firms. One of them, the Worcester-based SME Titania, which I visited recently, supplies software to customers in over 60 countries.

There's a huge potential market for UK cyber expertise and products abroad. I've discussed cyber security with my ministerial counterparts from countries as far afield as India and Israel, Spain and South Korea. It's clear that the phrase "Made in Britain" has enormous resonance. My message is simple – UK business is strong, competitive and innovative and is ready to work with you. Under our first ever Cyber Exports Strategy we aim to export £2bn worth of products and services by 2016, up from £850m last year.

We already punch above our weight in cyberspace and have the potential to become a 21st-century cyber superpower. Government and businesses must work together, so that we can all reap maximum benefit from the digital age.

*Francis Maude is minister for the Cabinet Office and Paymaster General*

Capgemini
CONSULTING.TECHNOLOGY.OUTSOURCING

# Cyber frontiers spur new controls

Michael Turner, security expert at Capgemini, explains how business can best overcome its vulnerability to technological attack

Technology's need for security is so obvious that it is almost not worth restating, but it still goes wrong and the landscape is changing beyond recognition. Mike Turner of Capgemini explains the issues to the *New Statesman*.

**Q** We keep hearing that the emergence of SMACT technology – Social, Mobile, Analytics, Cloud and the so-called Internet of Things – has changed the security landscape. Can you explain why these things are spoken about as if they were one thing?

**A** It's very easy shorthand when we discuss how cyber security has fundamentally changed.

It has changed because of the drivers around the uptake of cloud-based technologies; the adoption of mobile devices, be they smartphones or tablets; their capacity to carry social media; the move to being more mobile as a workforce; and the connection of everyday objects through the Internet of Things.

So it's a good shorthand and those five things have shifted the paradigm from the old "fortress" mentality of the keep and the castle, with a perimeter to defend. In the modern world, it's very difficult to define where that perimeter is. In a world of cloud services and mobile devices, many devices – such as phones, tablets and even laptops – will belong to a number of different stakeholders. Organisations may not have consciously outsourced their control but are finding that their security is now provided by cloud providers, or Apple, because it makes the iPhones the staff are using.

**Q** Is there a danger that some of the smaller enterprises might get a bit complacent about this? Many seem to think that because their data is in the cloud they are automatically backed up and virus-proofed, which is true only if their cloud provider is up to scratch.

**A** It's not really complacency. Things have become so complex that it's difficult to understand the range of issues. Before, you were faced with buying a range of services and putting them on your network. Now the integration issues as you start to adopt different technologies become quite significant. You wouldn't have to go far to find small to medium-sized enterprises using five or six different Software as a Service (SaaS) platforms or a cloud storage provider for their data, and they may be using multiple mobile devices.

On the other hand, the sheer amount of data means there can be a lot of it in what we might call a "data lake". One of my clients says if someone can break through their defences in such a complex environment then they probably deserve to take what they find, which is a little glib. If someone breaks through to an entire lake or reservoir of vital data they can do a great deal of damage.

**Q** So, if it's getting this complex, is outsourcing IT – and security – to a specialist company the best answer to stay safe?

**A** It makes huge amounts of sense to adopt SaaS services and cloud-based services. There are huge economic arguments that articulate the benefits of those. But organisations should be looking to do that only in areas that make sense, with a good understanding of the risks that they're adopting. At Capgemini we're great adopters of those sorts of technologies and we provide all of those cloud-based services.

We should understand that SMACT poses significant challenges; we see that in our own business and from our customers. However, we shouldn't be intimidated – those challenges are manageable. So my first advice to companies is not to be afraid to adopt those technologies but make sure you fully understand what you are undertaking.

It's becoming financially prohibitive to defend all of your information on mobile devices, the cloud and your own systems. You just can't guard every single place.

That means you need a clear view of the value of the assets you're trying to protect. The next piece is to align fully to the business strategy. Look at identity and access management, for example: a huge topic in the security world. How do you move from the old style of enterprise, where you'd manage identities of only your own staff, to where you're running an online business where you might be interfacing with millions of customers?

How well you manage that customer experience is likely to make the difference between whether those customers stay with you or not.

The third piece of advice is to have a clear strategy around where you're going to adopt these technologies. One of our customers is a national logistics firm, a very large organisation dealing with identities that run into millions, and it is using 20 cloud-based services, different SaaS providers accessed by a single portal. Interacting with all of those identities from the customers whilst integrating into the enterprise system where the invoicing and billing takes place is a major integration issue.

**Q** That's Identity and Access Management (IAM). What's SQAT?

**A** That's Security, Quality and Assurance Testing – and you can interchange "security" with "software".

One of the biggest challenges of the digital era is the rate of change in web applications and mobile applications. Commerce is changing at such a pace that the traditional life cycle – based around large waterfall projects, very clear requirements at the start of a project and a linear life cycle – has moved into the era of agile co-development: quickly deploying it, getting it out into the field as quickly as possible.

You've got to position that against the scale of the adversaries. One of the biggest developing areas is actually asking how to ensure that when you release some code developed in the last few hours, it's not immediately vulnerable to attack.

> **"In the modern world it's very hard to define where the perimeter is"**

We have a range of products as a systems integrator that we're able to bring to bear, whether it's the static testing of the code, or automatically looking for errors – or even dynamic coding, where you're pitching the types of threats and malicious code at a piece of code or an application to test its hardness. You also have to do it much earlier in a cost-effective way, and the only way to do that is to improve your coding quality.

The nub of it is that the rapid deployment of these technologies requires new ways of testing, new approaches; otherwise, it's going to be too late.

**Q** And are there advantages to having that testing done by someone external?

**A** Having a third party that hasn't developed the code doing the testing reduces the risk and brings some assurance. Development has to be rapid – the tooling has to be kept up to date, it has to be adapted quickly, and the adversaries are coming up with ever more novel ways of attacking applications.

If suddenly you're deploying a .net implementation in your organisation and haven't before, how are you suddenly going to get the skills to handle that?

**Q** How does an organisation like yours keep up?

**A** We make sure we have access to the latest thinking, whether at the intelligence end or the technology end. So we work very closely with the national authorities; we leverage and support all of the national initiatives around cyber security. The European Union is legislating now that each country has to have a cyber-response capability, so we've joined those organisations, the Cybersecurity Information Sharing Partnerships (CiSPs) internationally.

It's important as a global technology company that we're informing the debate as well as taking knowledge. At the other end of the scale, it's important that we're investing heavily in bringing into the company young talent – university graduates and apprentices who are not only informed, but using the technology. Incoming generations always evolve new ways of working with technology.

**Q** So how much of your work is managerial rather than technical? We still hear of people using weak passwords, encrypting sensitive information and then printing it out and leaving it in a hotel lobby . . .

**A** That comes back to my earlier point about having a comprehensive strategy. An example related to a national airport organisation that was implementing a very aggressive, very technologically advanced identity and access management regime, technology-based, two-factored, multifaceted. A significant proportion of the effort was over change management, and that was essential because they had to focus on the people as well as the megabytes.

There's an old adage that compliant in a technical sense doesn't necessarily mean secure – whether you're governed by Sarbanes-Oxley or another set of technical standards. If they're not backed up by awareness and processes, the weak link isn't necessarily the technical one. |

**For further information please visit: www.uk.capgemini.com**

# Protect and survive. Survive and thrive

In the face of cyber crime and theft of intellectual property, how can our government, business and industry protect the digital economy? The *New Statesman* brought some leading voices together to find out

Baroness (Lucy) Neville-Rolfe has been minister for intellectual property only since July but she is already well versed in the numbers that go with this particular policy patch. Creative industries contribute 1.6 million jobs to the UK economy, she notes, and IP-intensive industries represent 37 per cent of the country's GDP. "Britain has to compete on the world stage and we have to use the brains of our people and the strength of our education."

Neville-Rolfe – whose career spans the civil service, the prime minister's policy unit, a 16-year stint at Tesco supermarket in a variety of executive positions, and now minister and member of the House of Lords – was speaking at a *New Statesman* round-table debate last month, convened in partnership with the Federation Against Software Theft (Fast).

The title of the discussion, mirrored by the title of this supplement, was *Cyber Crime and IP Theft: Protecting the Digital Economy*, and Neville-Rolfe believes progress has been made. She pointed to the creation the Police IP Crime Unit (Pipcu), an overhaul of copyright law, a reformed IP Enterprise Court and "a much-improved legal framework, both civil and now criminal". However, she admitted there was much more to do. She described cyber crime as a "real threat to national security" and on IP theft, she said: "We know what it takes to protect our interests and we are alert to the needs and opportunities, but I believe passionately that we've got more to do."

## Size of the IP problem

So what is the extent of the issue she is looking to address? The Cabinet Office's Office of Cyber Security and Information Assurance agency estimates that cyber crime costs the UK economy £27bn a year. Of that, IP theft accounts for a third. Estimates are useful but calculating the impact of any grey or black market is notoriously difficult.

Assessing the impact of IP theft on the economy is not an easy task

As Neville-Rolfe pointed out: "Academics tend to come up with one set of figures and industry tends to come up with another, larger set of figures."

Putting a price on intellectual property theft is especially difficult, as any calculation which suggests that the retail value of illegally obtained software, music or film is equivalent to lost revenue is misleading. Some of those who have accessed illegal material would never have been purchasers in any case, while others go on to buy a legal version latterly, contributing to the digital economy rather than damaging it. Studies, including one from the European Commission Joint Research Centre in 2013, have shown this to be the case with music downloads.

Even the mighty Microsoft tacitly acknowledges the possible benign effects of piracy. In 2007, its business group president Jeff Raikes said: "If they're going to pirate somebody, we want it to be us rather than somebody else."

So while there is a discussion to be had about the morality – and criminality – of IP theft, assessing the direct impact on the digital economy is not a straightforward task. Alex Hilton, chief executive of Fast, accepted the broad point but insisted that an argument about numbers missed the bigger picture. "It's not just about the big guys [like Microsoft]," he said. Rather, it's about "the long-tail of smaller ⤶

ANNE KOEFOED

Table talk: personal and company data is at risk through a combination of human error and malicious intent bpi BRITISH PHONOGRAPHIC INDUSTRY

iab Internet Advertising Bureau UK

# Tackling cyber crime and piracy through creative partnerships

**NS: How big is the problem of piracy to the music industry in the UK?**

**BPI:** Online piracy is estimated to cost the UK's leading record industry more than £200 million per year – that's a huge sum of money that could alternatively be invested in new artists. At last count, more than 1 billion tracks were being illegally downloaded per year with around 6 million people in the UK engaging in file-sharing of all content every month.

**NS: Those are significant numbers. Would you say piracy is to blame for the decline in music sales and could this lead to the disappearance of the record label?**

**BPI:** Piracy has been a great challenge for the music and creative industries. However, 2013 was a strong year for music sales and revenues increased for the first time in four years by 1.9% largely due to the adoption of subscription and paid for digital music services. In the last digital decade, the music industry has transformed its business models and the way in which music is made available to fans.

So rather than the outlook being gloomy, we are cautiously optimistic for the future.

**NS: What is the music industry doing to reduce piracy?**

**BPI:** Our in-house Copyright Protection Unit works on behalf of musicians, labels and companies across the UK. We have sent more than 100 million take-down notices to search engines to request the removal of infringing content from search results; blocked 47 significant pirate sites in the UK; and launched a nationwide educational campaign called Creative Content UK. We are also working with the City of London Police's IP Crime Unit (PIPCU) and the advertising sector to reduce revenues from advertising on criminal sites.

**NS: You say you've been working with the PIPCU and the advertising industry, what progress have you made?**

**BPI:** PIPCU hosts a list of sites – known as the Infringing Website List, or 'IWL' - that they are investigating for IP crime, this is then made available to the advertising industry to limit advertising to the sites as part of their trading agreements.

**NS: How much do pirate sites have to gain?**

**IAB UK:** A report by the Digital Citizens Alliance calculated that advertising space on pirate sites could be worth $227 million in 2013 alone. Aside from the financial gains to be made, advertising can wrongly give these sites the appearance of legitimacy to the user.

It's important that advertisers, ad agencies and tech companies work with PIPCU to combat this issue.

**NS: How confident are you that the Infringing Website List can work?**

**IAB UK:** In the summer of 2013 we worked with PICPCU to trial the Infringing Website List (IWL). The results of that pilot scheme showed that the IWL had a positive impact overall. However, it is likely these sites will change behaviour to compensate for the lack of income so we need to remain vigilant.

**NS: How much interest has there been from the ad industry for this initiative?**

**IAB UK:** There has been a huge amount of interest from IAB UK members. Where an advert is found to be placed on sites with inappropriate or illegal content, the brand, its agency and other third parties can be put at huge reputational risk. As a result, ad tech companies have all been making individual efforts to tackle this problem.

The IWL provides us with a single authoritative source for identifying problem sites meaning ad tech companies are able to work collaboratively with their clients to limit brand advertising on illegal sites. It's a world first solution.

**NS: What next and where can interested companies find out more?**

**IAB UK:** We are actively signing up more advertising companies to support the initiative and taking proactive steps to give advertisers more control over their advertising online. Anyone interested in learning more should contact the BPI or the IAB UK directly. |

*__BPI__: www.bpi.co.uk – or contact*
*020 7803 1300 or antipiracy@bpi.co.uk*
*__BPI__ is the leading membership body for the UK's recorded music industry.*

*__IAB UK__: www.iabuk.net – or contact*
*020 7050 6964 or policy@iabuk.net*
*The __IAB UK__ is the trade association for digital advertising.*

developers who need to be more aware of some of the IP challenges. A lot of these guys are doing what they can just to keep the lights on . . . We're saving these businesses. That may sound trite but it is a genuine impact we're having."

Hilton's colleague Julian Heathcote Hobbins, deputy chairman and general counsel at Fast, added: "The problem with a discussion about numbers is that it ignores the times when you can save an IP-rich business that goes on to flourish and employ very many people."

## What is IP, anyway?

Neville-Rolfe said it is part of her mission to get people interested in the topic and make intellectual property something that everyone understands. One barrier in her way is that, beyond dictionary definitions of IP (see "Jargon buster", page 13), there is dispute about what it means in practice. Heathcote Hobbins, who posed the question "What is IP?" during the debate, noted: "I was always trained that there were no rights to an idea because that's what enables competition." His fellow lawyer Andrew Joint, commercial technology partner at Kemp Little, urged lawmakers not to look at IP purely in a copyright or patent context: "If we become very narrow in how we think about it then it gives people the room to exploit around the edges."

ANNE KOEFOED

Doug Davidson, director of cyber security services for Capgemini, agreed that a company's intellectual assets were now broader than had once been thought. "What we are seeing now is a mass attempt to extort the process," Davidson said – "everything from health and safety to business process. It's not just the idea, it's not the design or patent – it's the vast amount of supporting collateral that comes with the idea."

Meanwhile, Anders Jessen, head of the intellectual property unit in the Directorate General for Trade at the European Commission, observed that distinctions between IP and what he termed "trade secrets" presented a policymaking challenge at the European level. "There are ideas that a business could patent but decides not to, because part of the patent process puts the information [into the public domain]."

## The data problem

Perhaps the best way to illustrate the threat to intellectual property, in all its forms, is through example. Catriona Hammer, senior counsel IP at GE Healthcare, told the story of one former employee who downloaded many gigabytes of information on to four hard drives and mailed them to China where he had just accepted a job with a competitor.

"I only give you that as an example," Hammer said, "because you asked whether this is real. The answer is yes."

Leakage of valuable information need not be this dramatic. Julian David, chief executive of techUK, the industry association, pointed out that "employees on LinkedIn will describe a lot about themselves but also a lot about their company in so doing. And if you put two and two together you can see, for example, that there are a lot of new people in a particular department."

> "You can become rich if you protect your IP. It can all be stolen if you don't"

Whether malicious or unthinking, loss of IP is a distinct risk. "Any organisation nowadays relies upon data," said Hammer. "It's one of the most valuable assets and it's under threat daily. It's under threat from the cyber crime hacker. It's also under threat from employees, sometimes through carelessness and ignorance and sometimes deliberately stealing information."

## Strangling the pirates

If that is the problem, what are the potential solutions? Some prevention strategies are highly specific. For example, the government is talking to search providers including Google and Microsoft and urging them to relegate websites responsible for the illegal distribution of products and services further down the results pages and to push honest sites further up. According to Neville-Rolfe, the search engine auto complete function, which suggests likely search terms, is also prone to send web users to illegal sites. Talks about resolving the issue are ongoing, she said.

Other means of prevention are being pursued by the Police Intellectual Property Crime Unit, a 21-strong team that operates within the City of London Police and that was set up in 2013. Neville-Rolfe said she was pleased with its early successes: "Forty arrests in 12 months, 1.2 million of fakes seized and 3,000 illegal websites disrupted."

It is the disruption of websites selling counterfeit goods that is of particular interest to Detective Chief Inspector Daniel Medlycott. "The ability to strangle advertising and payments to the websites is key," he said. Medlycott's team created an infringing website list and encouraged leading brands to pull their advertising from those sites. Pipcu wrote to the top 100 brands operating in the UK; though the initial response was "fairly poor", today the majority comply with the request.

And in a twist, the police themselves began advertising on some of those infringing sites earlier this year. The banner adverts read: "This website has been reported to the police. Please close the browser containing this website."

## Education, education, perception

Medlycott reflected the views of a number of panellists around the table when he observed that parents who would normally understand the moral boundaries of theft in the physical world were ignoring or failing to appreciate similar boundaries in the digital world. "We still live in a society where the majority of parents will say, 'That's theft, that's wrong, don't do it.' With [IP theft] we don't have the support of the parents," he said. "We have people downloading music and thinking every musician is as rich as Bono."

This perception problem was recognised by the European Commission's Jessen, who said outreach programmes have proved problematic in the past but thought that attitudes may soon alter: "If you are buying a fake Rolex watch on a beach in Thailand you know what you are getting, even if you may have to buy another soon after.

"Now, people involved in these activities are moving into fake pharmaceuticals, health-care products – all sorts of things that we put on our body or in our mouth. And then I think people will start to develop a different perception of what kind of activity we are supporting."

Medlycott said Pipcu was talking to budding artists and musicians to explain how much damage illegally downloading material could do to their own future career. While he doubted whether these kinds of messages would be incorporated into the National Curriculum, they could at least be integrated into media studies, ICT and music lessons.

Neville-Rolfe said education in schools and beyond was "a job for us all". Alongside the right legal framework, the legitimate supply of goods and services and good enforcement, education was a key tenet in any strategy to combat IP theft. She pointed to new apprenticeships at GCHQ, a ten-step guide to cyber security aimed at business executives and the introduction of Moocs (massive open online courses) aimed at lawyers and accountants as evidence of the work the government was doing.

Neville-Rolfe said it was important to teach the risks of IP but "also the opportunities of building IP into your balance sheet. If you set up a fashion business, you can become rich if you protect your IP. And it can all be stolen if you don't." Kemp Little's Andrew Joint said those of the Facebook generation inclined to start their own business already understood the value of their creative endeavours. "There are always two things they are interested in when talking to lawyers," he said. "It's not data protection obligations or health and safety policies. It's their share options and how they protect their intellectual property. They realise that's how they monetise what they produce."

ANNE KOEFOED

### Good practice, bad practice

If education remains a critical component in tackling cyber crime and IP theft, common sense and good practice are important, too. GE Healthcare's Hammer urged companies, large and small, "to understand what data you've got and categorise it, because you don't want to treat all data in the same way. You will have some data that is really valuable – that's your secret sauce – and you want to make sure that that data is guarded, protected and shared appropriately. On the other hand, there is data where its entire value is in sharing it, increasing your reputation and attracting partners."

> "Understand the data you have and don't treat it all in the same way"

Davidson of Capgemini agreed. "I'm constantly bemused to the extreme why organisations don't understand their data better – don't understand it as an asset," he said. "I routinely come across companies that have no consideration to how they connect to third parties, no consideration to how they connect to different parts of the organisation."

Davidson also claimed that, with the possible exception of FTSE-100 companies, "cyber security is very rarely, if at all, in the risk registers of most organisations". This may come as a surprise, especially given pending EU data protection regulations that threaten penalties of up to €100m – or 5 per cent of annual global turnover – for breaches. It might be assumed that such fines would focus minds. Not so, said Davidson, who insisted he could point to a number of firms that say they are compliant when they are not. He added: "The perimeter within organisations has gone. There are only two aspects that allow an enterprise to control its domain. One is identity. Second is the API interface – the types of software and integration that you have around the organisation. The challenge that we have is not the big vendors with their software: it's rapid application development, it's people developing outside the organisation and introducing vulnerabilities."

On a practical level, Hammer noted that GE Healthcare had imposed restrictions on the use of portable media, including USB sticks. "Educating employees about the dangers is a step you can take, such as telling them not to lose sight of their laptop when they are going through airport security. Lots of laptops get stolen at airport security. So make sure you see it when it goes into the machine and make sure you see it when it comes out." Jessen added: "Businesses say to us that they now institute policies that mean when employees travel to certain parts of the world they can only bring in laptops that don't have sensitive data on them."

Fast's Alex Hilton injected a note of caution, arguing that preventing malicious behaviour was not always possible. "I've heard of organisations sticking Super Glue in USB drives [to prevent their use]," he said. "That's not a solution. You're never going to be able to police against individuals who just want to behave in this malicious manner. So for me, it's about education." He added that certain technologies were unfairly characterised as a security risk. "Cloud is not a negative, it's a positive . . . You've got better security there than you have in certain small-business scenarios." Did he include public cloud? "Absolutely," Hilton said, "because you've got levels of security. It's not just a free-for-all. It's about policy management and control."

### Let the market decide

This theme was taken up by Davidson. "Business has to be agile," he said. "Security is not the group that says no. It should be the group that says, 'OK.' " TechUK's Julian David suggested that industry was more likely to find solutions to security threats than lawmakers. "Letting the market have a big role here is very important because if you don't do that, you don't have scope for innovation and you risk fossilising things."

David pointed to two examples of industry involvement in action. He said his members were in conversation with the European Union about a cloud code of practice, while techUK had recently signed a memorandum of understanding with the US department of homeland security which may lead to UK technology companies creating products designed to protect security.

Joint agreed that industry had an important role to play. "Reliance just on laws isn't going to work, because laws take too long to get on the statute book, they happen at a slower pace than the technology itself. There has to be a suite of things – there has to be education and pressure of the industry to come up with solutions." He pointed to the introduction of digital rights management software into DVDs in the mid-2000s in an effort to address piracy. It was a move that was seen as draconian in some quarters. "Yes, it went too far," Joint said, "but the marketplace reacted to it."

The view was echoed by Heathcote Hobbins: "The industry, I would suggest, often has the fix because it has to." |

*This New Statesman round-table debate, in association with the Federation Against Software Theft, took place on 19 November 2014 at Portcullis House, adjoining the Palace of Westminster. For a full list of participants, see page two*

## Jargon buster

**Advanced persistent threat (APT)**
Long-term attacks that target specific organisations for economic or political motives.

**Copyright infringement**
See **Piracy**.

**Counterfeiting**
Defined by the Intellectual Property Office as "the manufacture, importation, distribution and sale of products which falsely carry the trademark of a genuine brand without permission and for gain or loss to another".

**Cyber crime**
A catch-all term to describe an array of criminal activities. Broadly, these fit into two categories: crimes unique to a technology environment, such as hacking and spreading malware; and those that use IT to facilitate existing criminal activity, such as distributing counterfeit goods.

**Denial-of-service attack**
An attack designed to render a website or network inoperable by bombarding it with traffic and messages. Inconvenience rather than theft is typically the objective.

**Hacking**
Gaining unauthorised access to a network, a website, a personal computer or smart device.

**Hacktivism**
Socially or politically motivated hacking.

**Identity theft**
The fraudulent access of someone's personal information with the intent of assuming that identity for malicious purposes and/or financial gain.

**Intellectual property (IP)**
Wipo (the World Intellectual Property Organisation) refers to IP as "creations of the mind". These include artistic work, names, images, symbols, logos and designs. Patents, copyrights and trademarks protect intellectual property under the law.

**IP crime**
Also known as criminal intellectual property rights infringement, IP crime includes counterfeiting and piracy.

**IP theft**
The theft of ideas, specifications, designs, and other secrets, processes and methodologies.

**Malware**
Catch-all term for malicious software, including Trojans, worms and viruses.

**Piracy**
Infringing the copyright of others' work by copying, distributing and/or importing those works. Such activity does not need to generate a profit to constitute a crime.

**Phishing**
The act of sending bogus emails or other communication in an effort to obtain personal information or access to secured networks, websites or messaging systems.

**Trojan**
An apparently legitimate program used for malicious intent: to gain access to a computer or network ahead of a future attack; to gain personal data; or to destroy or corrupt parts of a network immediately.

**Virus**
Code designed to infect a file and spread infection across a network. Infected machines are vulnerable to further attacks.

**Zero-day exploits**
Malware, including viruses that are as yet beyond the reach of antivirus software programs. |

*Sources: Intellectual Property Office; "The Cost of Cyber Crime" report for the Cabinet Office; Annual IP Crime report, 2013-2014; Crime Wales; Home Office Cyber Crime Strategy; Wipo*

CIPA
The Chartered Institute of Patent Attorneys

# Educating lawyers to help fight cyber theft

It's not just the IT department which can play a frontline role in the battle to protect the intellectual property which is the bedrock of success for many firms. Lawyers can play their part too…

Cyber security breaches are on the rise – particularly in Europe – making it increasingly important for businesses of all sizes to be vigilant in order to protect their intellectual property. Fortunately, there is an initiative to improve protection for Trade Secrets in Europe by introducing a directive that would require all EU member states to meet a minimum standard for protection of Trade Secrets.

A practical suggestion for all businesses is to understand what data they have, segment it and apply appropriate controls.

All data should not be treated in the same way. For example, companies will want to control and keep close track of their most valuable data – their "secret sauce".

But they will not wish to apply the same controls to all of their data and will have some they will want to share broadly to enhance their reputation.

Catriona Hammer (pictured), President of the Chartered Institute of Patent Attorneys and Senior IP Counsel, GE Healthcare, said: "IP theft and cyber crime is a growing threat to businesses large and small. IP professionals need to be aware of it and need to be ready to counsel their clients, whether internal or external.

"The discussion at the cyber crime and IP theft round table showed how complicated the issues are and that they need to be addressed on many different fronts – via legal and enforcement frameworks, education and new technical solutions.

**"This is a journey and, to a certain extent, we are at the beginning"**

"This is a journey and, to a certain extent, we are at the beginning. But the landscape continues to change very quickly and I would encourage all CIPA members to educate themselves about it. CIPA will, in future, be running some seminars on this topic."

The theft of IP and trade secrets is a very real issue for GE Healthcare. As reported in the Milwaukee Wisconsin Journal Sentinel and subsequently picked up by Bloomberg, a Chinese engineer who worked for a GE subsidiary in the USA stole more than 2 million files of trade secrets and other confidential company information and sent it to China. The estimated loss incurred by the company, based on the cost of developing the stolen information, was between $100 million and $200 million.

The engineer, Jun Xie, 41, agreed to a civil injunction ordering him to return what he could and cooperate with the company's investigation.

He is also awaiting sentencing on criminal charges and has reached an agreement with prosecutors to plead guilty to one count of stealing trade secrets. |

**CIPA JOINT CONFERENCE**
CIPA will hold a joint conference with UCL Institute of Brand and Innovation Law on the subject of Trade Secrets on 14 January 2015. The event will feature panel discussions between policy makers, industry experts and academics

**For further information please visit: www.cipa.org.uk**

# My job is to protect and promote your IP

*By Ed Vaizey*

Knowledge and intellectual property can help the UK become the most advanced digital economy in the world

I am proud of the UK's strengths in creativity, technology and innovation. Our economy benefits from the knowledge we have, the technologies we create and the creativity which goes into our cultural sectors. So while it is my job to promote this, it is also my job to protect it.

With world-renowned industries in the arts and sciences, and cutting-edge research and technologies, it is no wonder the UK is a target for those who want a piece of our success. Our intellectual property (IP) is valuable: IP-intensive industries generated an estimated 27 per cent of UK employment (7.8 million people) and 37 per cent (£512bn) of UK GDP in 2010. Whether it is online piracy, websites selling counterfeits or cyber attackers seeking to steal commercial secrets, it is vital that government and industry work together to counter the threat.

The scale of the threat is significant: 60 per cent of small businesses and 81 per cent of large organisations reported an information security breach in the past year. The average cost of the worst breaches runs into hundreds of thousands of pounds, sometimes millions for the larger firms. The threat comes from a wide range of actors, including criminals, hacktivists and state-sponsored groups. Although many cyber attacks are opportunistic and rely on the exploitation of poor IT set-ups and processes, there is also an advanced, persistent threat where sophisticated tools are being used for industrial espionage and to steal commercial secrets and IP. UK firms invest an estimated £127bn in knowledge assets, compared to £88bn in tangible assets, so it's easy to see how valuable this area is to our economy.

The news over recent years is littered with examples of stolen information, data assets and IP, with organisations as diverse as banks, public institutions, online retailers and manufacturers being targeted. Even well-known firms such as Google, Adobe and Yahoo! have not been immune.

Good cyber security can boost reputations and provide competitive edge

This is why the government is investing £860m in the National Cyber Security Programme, a five-year plan to protect and promote the UK in cyberspace. We're working with industry to raise awareness of the threat and encourage businesses to take action to protect themselves. The government's *Ten Steps to Cyber Security* guidance shows how organisations can manage cyber risk and protect their valuable assets, such as IP.

As a result of our work, many businesses in different sectors of the economy have become aware of the threat and are now responding well to the challenge. Our cyber health check of FTSE-350 firms showed 62 per cent of companies think their board members are now taking the cyber risk very seriously, and 60 per cent understand what their key information and data assets are. I recently launched a cyber security training package at the Law Society to provide professionals in the legal and accountancy sectors with the necessary cyber skills. We are also working to address the cyber threat with other sectors such as retail and finance.

The best thing businesses can do to protect themselves and their valuable IP is to understand their assets. Cyber Essentials, the new government-backed and industry-supported scheme, shows businesses how they can get the basics right and protect themselves against the most common cyber threats. The government is encouraging small and large businesses right across the economy to adopt Cyber Essentials and we now require suppliers who provide certain ICT products to hold Cyber Essentials certification. Certification allows organisations to display the Cyber Essentials badge, which demonstrates to customers and clients that they take cyber security seriously.

And this last point is key: it is important we see technology and security as an enabler, rather than merely a threat. As well as protecting assets and IP, good cyber security can boost reputations and provide a competitive selling point. And we see this more widely in how businesses are using technology to innovate and provide new products and services. The UK's digital sector now employs over one million people. Over the past ten years the ICT sector has grown over three times as fast as the whole economy. And in 2012, the sector contributed 8 per cent (£106bn) to the UK. The protection of our knowledge and intellectual property is absolutely crucial to this success and is a key feature of our work to make the UK the most advanced digital economy in the world. |

*Ed Vaizey is minister of state at the Department for Culture, Media and Sport and at the Department for Business, Innovation and Skills, with responsibility for digital industries*

UNIVERSITY OF
WEST LONDON
Ealing Law School

# LLM International Studies in Intellectual Property Law

At Ealing Law School our postgraduate courses provide you with a well-rounded, skills-based and professionally relevant education.

Intellectual Property (IP) is a fast growing area of the law, requiring highly qualified, multilingual specialists who can deal with IP rights across national borders.

The LLM International Studies in Intellectual Property Law course offers a specialised programme covering:

- Copyright, Trademark and Patent law including its European and international aspects
- Legal issues associated with new technologies, multimedia and cyberspace
- Strategic Management of Intellectual Property.

Taught by an experienced team, this course is designed for law graduates, practising lawyers and business professionals from anywhere in the world requiring a specialist legal and commercial expertise in technology and IP law.

Find out more and apply at
**uwl.ac.uk/pgIP**

**APPLY NOW. Places available for January and September 2015**