

SECURITY

Issue 3, 2013 • HK\$40

ASIA



Cover Story

The Devil in the Data

Leadership & Management

Hong Kong's Cave of Wonders

Legal Speak

New Competition Ordinance
Are You Prepared?



ISSN 2306-8781

Printed by R&R Publishing Ltd
Suite 705, 7/F Cheong K. Building,
84-86 Des Voeux Rd, Central, Hong Kong



A Knowledge Leader in Security

保安業智慧领航者

Specialized Guarding 專門護衛

Gurkha Officers 噶喀保安

Technology Solutions 保安科技方案

Mobile Patrol 巡邏服務

Key-Holding and Alarm Response 持匙服務及警鐘監控

Event Security 大型活動保安

VIP Protection 貼身護衛

Consulting and Investigation 保安顧問及調查服務

Phone: +852 21918918 Email: info@securitas.hk

www.securitas.hk





Circulation of Security Asia
Security Asia is delivered directly to the following associations and decision makers, throughout the Asia Pacific region, who are responsible for the purchasing of security related services products and services:

- Members of HKSA
- Government security bureaus
- Security consultants
- Law and accountancy firms
- Financial institutions
- Insurance companies
- Facilities management providers
- Security hardware and software manufacturers

Also available at:

- Security exhibitions
- Conferences and seminars
- Quality book stores



Published by R&R Publishing
Suite 705, 7th Floor
K. Cheong Building
84-86 Des Voeux Road Central
Hong Kong, SAR
Tel: (+852) 2126 7815
Info@RRPublishing.com.hk

www.RRPublishing.com.hk

Any opinions expressed in this publication are those of the author only and do not represent the opinion of the publisher, R&R Publishing. The publisher cannot be held responsible for any errors or inaccuracies provided by contributors or advertisers.

The publisher accepts no responsibility for any loss which may occur from such reliance.

The views herein are not necessarily shared by the staff or publisher.

The content of this publication is the property of the publisher and no part of this magazine may be produced without the written permission from the publisher. ©2013

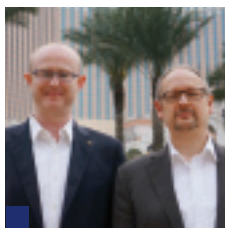
CONTENTS



4 COVER STORY
THE DEVIL IN THE DATA – We look at the techniques employed by governments to collect personal data and what they do with it. Has Edward Snowden done us a favour by exposing what governments are up to?

10 LEADERSHIP AND MANAGEMENT

HONG KONG'S CAVE OF WONDERS – Malca-Amit are leaders at transporting and storing valuable goods from diamonds to works of art. We talk to General Manager Ido Tomasis to see how they do it.



14 SURVEILLANCE
GERMAN CCTV COMPANY HITS JACKPOT IN MACAU'S CASINOS – German company Dallmeier seems to have taken the lead in providing the most extensive IP-based video systems to the casino's of Macau.

18 CYBER SECURITY
BASIC PC PROTECTION FOR TECHNOPHOBES – Top 10 security tips for your computer from the Information Services and Technology Department of the Massachusetts Institute of Technology.



- 3 HKSA** – Message from the HKSA Chairman
- 12 LEGAL** – New competition Ordinance
- 16 LOOKING AHEAD** – Top 10 security threats for 2014
- 20 IN THE NEWS** – Latest issues from around the Asia-Pacific region
- 22 WORLD FOCUS** – Latest issues from around the world
- 24 THE BACK PAGE** – A satirical look at security



The Hong Kong Security Association and our members are dedicated to provide and maintain the best service and product standards.

The Hong Kong Security Association was founded in 1984 and is the only Association of companies holding security licenses issued by the Security and Guarding Services Industry Authority.

Our member companies are principally engaged in providing many different aspects of security services:

- ▲ **Guarding services-commercial and residential.**
- ▲ **Cash transport services by armoured vehicle.**
- ▲ **Installation and maintenance of alarm systems and equipment.**
- ▲ **Remote monitoring of alarms, fire alarm and CCTV systems.**
- ▲ **Supply of security systems and products.**
- ▲ **Investigation and security consultancy services.**

The Association works with the Security & Guarding Services Industry Authority for the regulation of the industry.

The Association works closely with the Security Companies Inspection Unit of the Crime Prevention Bureau of the Hong Kong Police Force.

The Association, being a member of the Security Services Training Board of the Vocational Training Council contributes towards quality framework and training standards.

The Association forms working groups to tackle assignments and special projects.

The Association holds social functions to provide platforms for idea sharing and opportunity for members to meet.

Raising the standards within the Security Industry

MESSAGE FROM THE HKSA CHAIRMAN

By Douglas Renwick

This year has seen a number of exciting activities in the Hong Kong security industry – including the launch of a new Security magazine “*SecurityAsia*”, The Hong Kong Security Association’s subtle re-branding and the launch of the Association’s new website.

The membership numbers of the Hong Kong Security Association continue to grow, which is highly encouraging. Our collective voice is used to raise issues with the Security Authority, Police, Labour Department and other Government bodies. These assist with the Association’s aim to continually looking at opportunities to improve and raise standards within the Security Industry and tackle head-on the issues that affect our industry now and in the future.

The Government’s Policy Study on Standard Working Hours has been published and the Standard Working Hours Committee has convened. The Association is working diligently to ensure our industry related issues are heard and considered.

Manpower and labour issues continue to blight the security industry – under the current importation of labour scheme there is not a viable option to swell the ranks of the security industry. The security companies, end users, customers and Government must sit up and take-stock. The short term affect is salaries will continue to rise as the lack of manpower continues to affect Hong



Kong in general and more especially in the Security industry.

To combat the increases, service charges and staff salaries must follow suit. Many companies already operate on a very low profit margin, therefore increasing salaries and charge rates must be considered as a viable option. While looking at options to attract people to work in the security industry... including pay and conditions, working hours and garnering additional respect for the work conducted.

The Hong Kong Government infrastructure projects, expansion of Macau casinos and the overall general increase in construction projects are forecast to continue well beyond 2014.

So as an industry we need to act now to ensure our talented manpower can be retained.

On a lighter note, The Hong Kong Security Association will be celebrating its 30th (Pearl) Anniversary in 2014 so keep a look out for the association’s activities. There will be a Anniversary publication to celebrate the Association’s activities over the last 30 years - I encourage you to use the opportunity to tell your anecdotes, share your experience with the Association and to also advertise in the publication to ensure you promote your companies products and services to your target market.

Merry Christmas & Happy New Year 2014 ■

THE DEVIL IN THE DATA



Modern communication systems are not only convenient for everyday users.

They also enable governments and corporations to trawl through the Big Data of emails, phone calls and internet logs to understand more – perhaps more than they should – about the activity of their citizens and customers.



The information age, as we are all now fully aware, is also the information-gathering age.

There has never been so much information about what people are doing, or more interest in harvesting and recording that information. Communication technologies have become all-pervasive, and every interaction, whether by phone, mobile network or the internet, is an opportunity for those with the right technology and enough incentive to learn something, however small, about the behaviour of groups or individuals.

The motivation for doing so varies. Governments view us as citizens or taxpayers or voters – but also as potential criminals or threats to national security. Corporations see us as customers, or potential customers. Thus businesses are more interested in understanding patterns of behaviour and, from them, interpreting our likely future purchasing choices. Governments, on the other hand, are more concerned with sifting through the infinite haystack of communications in search of rare needles of value – intelligence uncovering a terrorist plot, for example, or evidence of illegal activity.

Revelations about the mass surveillance activities of the US National Security Agency (NSA) by

whistleblower Edward Snowden have added new levels of detail to what we already knew, or at least assumed, about government monitoring practices. The revelations have centred on the NSA and to a lesser extent its British equivalent, GCHQ. However, there is no doubt that other governments with highly developed security apparatuses are employing similar tactics of blanket monitoring combined selectively with more intensive surveillance.

Layers of observation

When it comes to monitoring emails and similar internet traffic, the NSA uses sophisticated computer programs that act as a filter, automatically scanning billions of emails and flagging up those which contain suspicious content. In particular, the NSA has been operating a program called Xkeyscore, which unselectively records everything from Google searches to Facebook posts. In much the same way, it uses complex algorithms to scan billions of phone calls for key word combinations. Governments are particularly interested in the metadata attached to these communications – not the contents themselves, so much as related information such as the identity of the callers, and call duration. Such operations are termed “massive intercepts”, and target entire populations.

The efficacy, never mind the

legality, of wholesale data sweeps has inevitably been called into question. After a decade of massive intercepts, it appears that the US government obtained information that helped it to prevent a terrorist attack on just one or two occasions. Moreover, in some cases US intelligence agencies were in possession of data which might have been used to trace terrorists, but they missed the vital clues because of failures in analysis – because they had too much information to sort through, in other words. Even so, the US government still appears to value this broad-brush tactic. In new legislation brought in response to public concern over mass data

user data about specific individuals from major tech players such as Apple, Facebook, Google and Microsoft. Facebook, for example, reported that it has handed over the private data of around 19,000 individuals at the request of intelligence and law enforcement agencies.

Bruce Schneier, a commentator on security and surveillance practices, has termed this the “public/private surveillance partnership”. Tech firms on whose services we all rely on a daily basis have access to their customers’ personal data, which they undertake to keep private; but then they share it with governments without their customers’ permission in the name

global market for surveillance systems grew from zero to \$5 billion annually, as governments around the world grew increasingly interested in private-sector solutions that would allow them to monitor their citizens’ activities. That market remains strong in spite of Snowden. But now, in the face of customer outrage over the sharing of personal data, companies also see a business opportunity in investing in technologies which aim to defeat government snooping efforts. This raises the prospect of a private-sector surveillance arms race, with ever-improving monitoring systems on one side and countermeasures on the other.

For example, one standard approach to protecting data communications is to encrypt emails (Secure-

In the decade after 9/11, the global market for surveillance systems grew from zero to \$5 billion annually, as governments around the world grew increasingly interested in private-sector solutions that would allow them to monitor their citizens’ activities.

collection, a new FISA Improvements Act – FISA being the pre-existing Foreign Intelligence Surveillance Act – banned “the collection of bulk communication records” except in certain circumstances, from which critics inferred that massive intercepts would probably continue.

However, more targeted surveillance naturally requires smarter technology, more manpower – and quite possibly cooperation from third parties.

This is where governments have turned to the private sector. It’s now clear that the US and other governments monitor the activities of individuals with the assistance – sometimes offered willingly, sometimes reluctantly – of big technology companies. The NSA’s notorious PRISM program, which Snowden uncovered, is one such effort: through PRISM, the NSA has been obtaining supposedly privileged

of national security. This alliance, Schneier argues, “allows both the government and corporations to get away with things they couldn’t otherwise”, because both parties get access to huge amounts of data, and neither side is motivated to back legislation to restrict its collection.

However, the backlash against NSA surveillance has resulted in a surprising bifurcation of the surveillance market, with some companies working to support government surveillance and others now working to obstruct it. Some companies now realize that there is a reputational “cost to co-operating” with government surveillance programs, according to Schneier.

In the decade after 9/11, the

Socket Layer encryption, or SSL, is the most common system). In the wake of the NSA scandal, major email service providers that didn’t already encrypt their users’ messages, such as Google and Yahoo, announced that they would introduce SSL encryption to their email offerings. This certainly makes it a lot more difficult for governments or other parties to monitor email communications. In November, Yahoo confirmed that it was moving ahead with its encryption strategy, effectively confirming that it valued the trust of its users over the trust of government intelligence agencies. Meanwhile, Google underlined the growing sense of industry opposition to the government when Eric Grosse, the company’s vice president for security engineering,



confirmed Google's own encryption plans in September, characterising the emerging technology struggle as an "arms race" in which "government agencies [are] among the most skilled players in the game".

However, there are off-the-shelf products which can crack SSL and other forms of encryption. US firm Blue Coat Systems is the market leader of this type of solution; its ProxySG system can decrypt any SSL communications and relay the decoded messages to a third party, which would most likely be a government or law enforcement agency. The company did not respond to requests for comment, but in May it was widely reported that the Syrian government had obtained Blue Coat Systems' technology and was using it to monitor internet traffic. And if Syria has managed to acquire this type of capability, it seems likely that many others have done so, too.

This is leading some messaging providers to go even further. Specialist

providers of secure email services have of course seen their business models challenged by government court orders demanding that they hand over security keys in order to facilitate surveillance activities. One such provider, Lavabit, shuttered its service in the summer when the US government demanded access specifically so that it could monitor the communications of Edward Snowden, a Lavabit customer. Another secure email provider Sient Circle then followed suit.

However, Lavabit founder Ladar Levison is now working on a new initiative with Silent Circle, called Dark Mail, which will offer an improved version of the companies' secure protocols as open-source code, encouraging encryption to be adopted more widely. While it will still be possible to crack encrypted messages, Levison argues that mass surveillance will become extremely difficult if most emails are sent securely. Meanwhile,

the question of the legality of the government's insistence that Lavabit hand over its security keys continues to be addressed in the courts, with potentially far-reaching implications for future surveillance activities.

The problem with encrypted communications, though, is that they arouse the suspicion of governments and law enforcement agencies, whose natural inclination is to wonder what the users of encrypted systems have to hide. It is alleged that governments routinely intercept and store encrypted communications, even when they are unable to crack them, with a view to revisiting and decoding them if necessary at a later date.

So encryption is not bullet proof, and neither, it seems, are other, simpler means of avoiding government surveillance. Most cell phone users are aware that their phone, when switched on, can be tracked because the device broadcasts its location within the network. But it has recently



emerged that governments have developed ways of tracking mobile devices even when they are switched off. The method remains classified, but security analysts assume that the process involves the uploading of malware to a phone which a law enforcement agency wishes to track; this malware then ensures that the phone's broadcast functions remain active, even when it appears to be switched off.

The legality of hacking into phones in this way is murky at best. In the same way, we tend to regard computer hacking as a criminal activity – and yet there is a thriving, legal market in the development and sale of 'exploits', which are essentially off-the-shelf hacking solutions. French cyber-developer Vupen is one example of a company which markets offensive exploits, though only, it stresses, to "trusted countries and government agencies". These offensive exploits could have a number of purposes, but in many cases they will be used to monitor supposedly secure systems, and relay sensitive data to the

individual or organisation responsible for deploying it.

The simple conclusion, as articulated by FBI intelligence analyst-turned-commentator Tim Clemente, is that "no digital communication is secure". Or, as Ladar Levison concluded after pulling the plug on Lavabit: "I'm taking a break from email. If you knew what I know about email, you might not use it either."

Corporate surveillance

If governments need to access our communications through secretive and legally questionable means, businesses have a far simpler mechanism for obtaining our data. We give it to them, freely.

It stands to reason that the providers of services such as email, internet and telephony should be privy to their customers' communications, as well as personal data and billing information. And while we generate huge volumes of data – Big Data, as analysis companies describe it – simply by spending time online, for

example, it's easy to assume that this information has no value, and would not be of interest to any third parties.

However, this is far from the case. Tracking cookies have been commonly deployed for years now by internet companies interested in learning more about user habits: these are programmes uploaded to your computer, often without your knowledge, which send back information to their originators about your usage and browsing patterns. This is why banner ads for flights to Tokyo, for example, will suddenly appear on websites you visit, if you've recently been searching online for information about Tokyo. Indeed, some sites will install several dozen cookies onto your computer to track various different types of behaviour.

But this description does not do justice to the level of analysis which some businesses now apply to the monitoring of browsing habits. By closely monitoring user activity, data metrics companies are able to provide clients with a detailed picture of the

digital marketplace. However, even here there are different levels of analysis. As John Jordan, a professor at Penn State University who specialises in the study of business information systems, puts it, “just because something can be measured doesn’t mean it should be measured”. Thus corporations, just like governments, are discovering that the collection of too much information can damage their public image.

The most important distinction is whether the collected data is personally identifiable information (PII). In one sense, this is the big difference between government monitoring and business monitoring: the data is not much use to governments unless they can link the activity to specific

This is enough granularity for most advertisers: ads placed in this way are still much more targeted and effective than an advertiser buying commercial airtime on TV, for example. It also enables both the data collection company and the advertiser to claim that they are not invading anybody’s privacy. Most monitoring companies like eXelate also have opt-out functions, which will block targeted ads on a particular computer.

Axiom, another data-technology firm, has taken audience reassurance a step further, launching AboutTheData.com, a site where concerned individuals can learn more about data collection in general, and also discover what kind of information Axiom has collected about them specifically, and

be the new battleground for internet privacy, as campaigners argue for bans on the collection of any data beyond non-specific non-PII. This is when Big Data can become too big to handle, as Jordan warns, as companies drown in “numerical tsunamis” and lose sight of the “basics of sound analytical practice”.

Many internet users who do not want to be tracked at all subscribe to Virtual Private Network (VPN) services, which use special internet protocols which make it appear as if they are accessing the web from a different city or country. However, this has inevitably put VPNs in the regulatory spotlight. Some VPNs have hit back against government attempts to access their users’ data by simply not storing any. However, the EU, for example, introduced a Data Retention Directive several years ago which forces companies such as email

While many end users do not bother to opt out of non-PII data-gathering schemes, or visit sites that can provide details of the way they are being tracked, most people are uncomfortable with the idea of PII being collected and sold onto third parties.

individuals; but businesses do not necessarily need PII, since they are interested in general usage patterns, or in marketing products to the right type of customer, though not necessarily to particular individuals.

US-based monitoring firm eXelate is one of a growing number of specialist online data collectors which gather non-PII. The company’s approach is to partner with a range of popular websites; these websites then upload a tracking cookie to computers from which they were accessed. Via the cookies, eXelate gathers data about internet usage on a particular computer, but it does not know the identity of the person or persons using that computer. Its clients are then able to target advertising campaigns at the right end users, even though they don’t know those end users’ identities.

how that data is being used.

While many end users do not bother to opt out of non-PII data-gathering schemes, or visit sites that can provide details of the way they are being tracked, most people are uncomfortable with the idea of PII being collected and sold onto third parties. However, many data-tracking companies are pushing the envelope of what qualifies as non-PII. Though omitting individual users’ names, they may compile profiles of individuals that include many other personal details, such as sex, age and marital status, or even record user activity, such as keystrokes. This sort of monitoring practice is likely to

service providers to retain all web and email logs for a certain period of time, for law-enforcement purposes. VPNs continue to argue that they are not covered by this type of legislation, but it is clear that governments intend to challenge the ability of VPNs to undermine their surveillance efforts.

Both governments and corporations are therefore still coming to terms with the information-gathering age of Big Data. The next step will be to gather more selectively – to get the Right Data – and then use it more smartly and more equitably than they are doing today. Otherwise, the citizen and customer backlash will only gather pace. ■

Hong Kong's Cave of Wonders

Malca-Amit began business in 1963 providing export papers for valuables from a small office in Tel Aviv, Israel. Fifty years on, the company is now a global concern headquartered in Hong Kong. It specialises in tailor-made solutions to the secure transportation and storage of gemstones, precious metals and fine arts. *Security Asia* visited Malca-Amit's new facility in Hong Kong for a first-hand look at how they keep billions of dollars' worth of gold and fine arts hidden from prying eyes.



Construction began on Asia's largest private secure storage facility in February 2012, at significant but undisclosed cost. Spanning two ground floor units of a Chek Lap Kok commercial building, the vault took five months to build using 264 tonnes of reinforced steel and some 600 cubic metres of cement.

Essentially, the vault comprises discrete units within the original units. This state-of-the-art facility is designed, constructed and managed by Malca-Amit and so discreet that it took *Security Asia* staff a while to find the entrance, to the evident amusement of observers in the control room.

In fact there are five vaults: a

common vault, a diamond vault, two smaller vaults for the use of major financial institutions and a vault specifically designed for storing fine arts and collectibles. The fine art vault is a first for Hong Kong we are told, as it combines full vault security with climate control and FM 200 fire suppression. Each vault has a colour-

coded floor for instant recognition by CCTV operatives in the control room. Security levels escalate as we approach the vault area, with dual and triple access control systems in place.

Security manager Mr Erez Bergman explains that the facility aims to provide a high level of customer hospitality as well as the utmost security. What is immediately noticeable is the near-soundlessness of the interior compared to the noise and traffic outside. We are shown the viewing room where customers may inspect their valuables; it is comfortably appointed with a couple of white leather chairs and a simple table against the far wall supporting weighing scales and a pair of anglepoise desk lamps. Above the table is a high-resolution CCTV camera which can be disabled at the request of the customer.

Mr Ido Tomasis, General Manager of Malca-Amit Secure Logistics Ltd., adds that the company's global network constantly tracks every item in transit and can swiftly make the necessary arrangements if, for example, an aircraft is diverted from its flight plan. Moreover, customers are given access to a secure web portal which updates them with live feeds from Malca-Amit's global IT



System Inventory.

Security Asia can confirm the shotguns carried on the armoured trucks are not merely for show; we visit the armoury, fitted out with strengthened, absorbent walls and blast-proof light fittings. Erez is proud to note that the company not only meets the Hong Kong Police Force's stringent security and safety requirements, but often exceeds them. The guards undergo three weeks of training and need to pass the requisite police tests before taking on their roles. As first-

line representatives of the company they are required to be smart and courteous at all times.

There is a general movement of physical gold from west to east and the company is utilising its existing network and investing heavily in hardware to capitalise on this trend. China's gold imports for the first half of 2013 were over 706 tonnes, up 54% from the same period the previous year, according to the China Gold Association. The number of wealthy individuals in the region has also grown considerably and Malca-Amit recently opened a 200 tonne silver vault in Singapore, adding to the firm's five existing gold vaults in the Freeport district. A new facility – which will overtake Hong Kong to become the largest in Asia - is soon to open in Shanghai and the company plans further expansion in the region to cope with the rising demand for secure storage.

Malca-Amit currently employs over 150 staff in Hong Kong and this number is expected to increase 30-40% by the end of the year. The company's armoured vehicles will soon become a more familiar sight on the city's streets and we can only speculate on what treasures they may transport. ■



HONG KONG'S NEW COMPETITION ORDINANCE : **ARE YOU PREPARED?**

A healthy and efficient economy is the cornerstone of an international financial centre and it is somewhat curious (albeit some commentators have said that there was already healthy competition in Hong Kong) that, until recently, Hong Kong did not have a competition law. That changed in June 2012 when the Competition Ordinance was enacted. If you are an entity, and this includes an individual, engaging in economic activity, you will be considered an "undertaking" and potentially subject to the new competition regime, so you need to understand what this new regime may mean for you.

First Conduct Rule and Second Conduct Rule

The Ordinance prohibits anti-competitive conduct pursuant to two main rules: the First Conduct Rule and the Second Conduct Rule. The First Conduct Rule is likely to be of most interest to Hong Kong businesses as it prohibits any agreement, concerted practice or decision of an association of undertakings, the object or effect of which, is to prevent, restrict or distort competition. The main thrust of this rule is to prohibit competitors colluding with each other in an anti-competitive manner (such as agreements, etc. are sometimes known as "horizontal agreements"). In addition, it will also catch agreements, etc. with counterparties such as

suppliers and distributors who operate at different levels in a production or distribution chain (so-called "vertical agreements").

Most jurisdictions with competition laws have similar provisions; what is slightly unusual about Hong Kong's regime is that it divides this into two categories: serious anti-competitive conduct (which is specified as price fixing, bid rigging, output restriction and market sharing) and non-serious anti-competitive conduct. For non-serious anti-competitive conduct, there is a lighter touch to the regulatory regime, which we mention below.

The Second Conduct Rule prohibits the abuse of substantial market power that has the object or effect of preventing, restricting or distorting competition.

There is a third rule which is of limited application; this is the merger control rule which prohibits mergers and acquisitions, in the telecommunication industry, that substantially lessens competition in Hong Kong.

Exemptions and exclusions

To address the concerns of small and medium-sized enterprises, there are some entities

who will be exempt from the First Conduct Rule and the Second Conduct rule. The First Conduct Rule will not apply to any agreement,

concerted practice or decision where the combined turnover of the undertakings involved is less or equal to HK\$200 million. The Second Conduct Rule will not apply to any undertaking with a turnover of less than or equal to HK\$40 million.

There are also a number of other exemptions and exclusions, see the summary table on facing page.

Competition Commission and Competition Tribunal

Two bodies have been established: the Competition Commission and the Competition Tribunal. The Chairperson of the Commission is Ms Anna Wu (who is currently a non-official member of the Executive Council of Hong Kong and Chairperson of the Equal Opportunities Commission and who previously held the position of Chairperson of the Hong Kong Consumer Council) and there are 13 other members of the Commission who are comprised of representatives from various industries. Every Judge of the Court of First Instance is a member of the Competition Tribunal and the current President of the Competition Tribunal is the Honourable Mr Justice Godfrey Lam Wan-ho.

The Competition Commission has wide powers of investigation and it will be able to settle cases without bringing proceedings before the Competition Tribunal. However, it is the Competition Tribunal who has

the power to impose the more severe penalties, including a fine of up to 10% of a business's annual turnover for 3 years (much debated during the legislative process), restraining or prohibition orders, orders requiring agreements to be modified or terminated disqualification orders of up to 5 years against directors and so on.

As part of its broad investigation and enforcement powers, the Competition Commission will be able to search premises and seize documents, require the production of documents and require persons to attend interviews. It can issue infringement notices for alleged serious anti-competitive conduct and abuse of substantial market power, accept commitments (where a person agrees to take action or refrain from taking action which is potentially anti-competitive) and enter into leniency agreements (where a person receives no or reduced penalties in exchange for co-operation). The Commission can accept complaints from anyone; it may however refuse to investigate if it considers it reasonable not to do so, and in particular, where the complaint is trivial, vexatious or lacking in substance.

For a case involving non-serious anti-competitive conduct, the Commission is able to issue an entity with a warning notice, instead of an infringement notice. If the entity ceases the alleged anti-competitive conduct within the period specified in the notice, then no further action is taken.

In addition, anyone who has suffered loss or damage from anti-competitive conduct may bring follow-on action for civil damages.

So, what does this mean for you?

So what does this mean for security professionals? With a new regulator in

Hong Kong, it is inevitable that there will be inquiries and investigations where professionals, such as forensic experts and seasoned investigators can assist companies who are concerned about anti-competitive conduct within their organisations, with competitors or counterparties.

Security professionals should also look at their own internal practices: are any of them potentially anti-competitive? Are there, for example, regular exchanges about prices or joint bids for particular projects? Is your organisation likely to have "substantial market power"? A first step is to raise awareness within your company and assess whether the law applies to you. If it does, or potentially it does, then you may want to review your current agreements and practices for potential anti-competitive issues and assess if one of the exemptions or exclusions apply. Many companies are also beginning to establish

compliance programmes. The good news is that you have time: although the law has been passed, it is not yet in effect and not likely to be in effect until early 2015. In 2014, we expect the Competition Commission to be busy recruiting key personnel, drafting guidelines and consulting with various industries and the public. Many of the competition issues that will be faced are not straightforward and will require careful analysis; whilst we expect the Competition Commission to issue guidelines to assist businesses in Hong Kong, nevertheless businesses should be pro-active and start appropriate preparations. ■

JILL WONG, Partner, Howse Williams Bowers

This article is only a general outline. It is not legal advice. You should seek professional advice before taking any action based on its contents.

Type	Applicable to First Conduct Rule	Applicable to Second Conduct Rule
Block Exemption	Yes	No
Efficiency exclusion - an agreement that improves production, distribution, technical or economic progress, and benefits consumers	Yes	No
Public policy grounds	Yes	Yes
To avoid conflict with international obligations	Yes	Yes
For compliance with a legal requirement	Yes	Yes
Provision of services of general economic interest by an undertaking entrusted to do so by the Hong Kong Government	Yes	Yes

German CCTV company hits the jackpot in Macau's casinos

Macau, a one hour ferry ride from Hong Kong, has emerged as the most popular gambling destination on the planet – and is one of the most important sales markets for Dallmeier. Not only has the German video surveillance company designed and installed the most extensive IP-based video systems in the world here, it has also operated its own company branch on the island for several years.

Until 1999, Macau was a Portuguese colony, and its European heritage is still clearly on display in its

architecture and street names. Today, the province is a Special Administrative Zone of the People's Republic of China. Macau is also heavily influenced by its Asian identity, even though the city skyline is dominated by its enormous casino and hotel resorts.

Unlike in China, gambling is not forbidden in Macau, and has thus become one of the largest sources of revenue for the province. The foundation was laid for the industry by one gargantuan construction project: the two offshore islands of Coloane and Taipa were joined by

man-made landfill. On a 1.8 mile stretch of artificially constructed land a skilfully planned gaming paradise of unimaginable proportions took shape – the Cotai Strip. Elaborate, imaginatively designed resort complexes now make gamblers' pulses race and have helped the Cotai Strip to surpass the magnetic powers of even its model Las Vegas.

The success story for Dallmeier - active in the casino industry since 1997 - began in 2003, when with an international tender the first foreign casino in Macau, the Las Vegas Sands,



Dallmeier's Craig Graham, General Manager, Asia Region and Konrad Hechtbauer, Director, Project & Applications

was looking for a surveillance system. Konrad Hechtbauer, Director Project & Applications at Dallmeier, looks back: “Dallmeier established itself in Macau about 10 years ago, with the first digital video solution and about 1200 channels.”

But this first order from the Sands was only the beginning: just a year after it opened, the casino doubled its capacity – and of course this also meant that the surveillance system had to be expanded correspondingly. As the boom in Macau continued unabated, so the Sands Group grew too, and over time it acquired several more properties on the main island of Macau as well as on the Cotai Strip. By this time, the Sands, the Venetian and the surrounding hotel complexes had combined to form a single interconnected network. A staggering 15,000 cameras here are controlled from a main control centre!

Many more projects, such as the City of Dreams with approximately 5,000 cameras, have followed over the years. And the end of the development is nowhere in sight yet: not only are new casino and hotel resorts being built; the existing casinos are constantly expanding their video systems.

Konrad Hechtbauer explains: “The systems are becoming bigger and bigger, and more and more complex. They now also incorporate a multitude of interface connections, such as card readers, slot machines or POS systems. The data from the peripheral systems is linked to the video images. The user is alerted to sensitive areas automatically by complex mathematical calculations, so the system functions proactively. Unusual situations at the gaming tables are detected and reported by means of intelligent video analysis. Our many years of experience in Macau are incorporated systematically in our development programme, and as a result Dallmeier is constantly able to



present new innovations.”

In order to satisfy the many specifications by its customers in Macau, Dallmeier has founded its own subsidiary: Dallmeier International, a joint venture between Dallmeier in Germany and its Australian business partner C.R. Kennedy.


Stephen Beard, Managing Director Dallmeier International, says: “I remember the first discussions

for the long term.

Craig Graham, General Manager Asia Region at Dallmeier International, explains: “In our office we have eight staff, seven of them engineers, and we do repair work within the office and also at clients’ sites. We also have a warehouse and store room here servicing our

major clients. In total we service over 20,000 channels across Macau and also in the region.”

In a purpose-built showroom, the latest developments can be tested and demonstrated to customers. One of the most radical new innovations is the patented Panomera® camera technology, which offers hitherto inconceivable resolution and image quality thanks to a completely new

 *By this time, the Sands, the Venetian and the surrounding hotel complexes had combined to form a single interconnected network. A staggering 15,000 cameras here are controlled from a main control centre!*

about our joint venture which really stemmed from the fact that C.R. Kennedy, our company in Australia, was instrumental in the first digital system ever in a casino surveillance system. The job went so well that Dallmeier and C.R. Kennedy decided to join a joint venture in Hong Kong and later into Macau to provide Dallmeier systems to the new Western casinos that were going up rapidly.”

From consulting and planning for the system to commissioning and including after sales service, Dallmeier attaches great importance to supporting its customers as a partner

lens and sensor concept – in real time and at up to 30fps.

From the office in Macau, all casinos can be reached in 20 minutes or less, so professional Dallmeier personnel can be on site almost immediately to assist with emergencies, provide support and for all ongoing expansions.

Craig Graham recalls the beginning of the office: “I remember when we first opened the office Stephen said that the opposition claimed we would never get any business within Macau. Here we are ten years later with one of the largest presences in Macau’s CCTV industry. ■

ISF's top security threats for 2014

The Information Security Forum is the world's leading authority on information risk management. Here Steve Durbin, global vice president of the ISF, identifies the top security threats for 2014.

1. BYOD trends in the workplace

As the trend of employees bringing mobile devices into the workplace grows, businesses of all sizes continue to see information security risks being exploited. These risks stem from both internal and external threats, including mismanagement of the device itself, external manipulation of software vulnerabilities and the deployment of poorly tested, unreliable business applications.

If the Bring Your Own Device (BYOD) risks are too high for your organisation today, stay abreast of developments. If the risks are acceptable, ensure your BYOD program is in place and well structured. Keep in mind that a poorly implemented personal device strategy in the workplace could face accidental disclosures due to loss of boundary between work and personal data and more business information being held in unprotected manner on consumer devices.

2. Data privacy in the cloud

While the cost and efficiency benefits of cloud computing services are clear,

organisations cannot afford to delay getting to grips with their information security implications. In moving their sensitive data to the cloud, all organisations must know whether the information they are holding about an individual is personally identifiable information (PII) and therefore needs adequate protection.

Most governments have already created, or are in the process of developing, regulations that impose conditions on the protection and use of PII, with penalties for businesses that fail to adequately protect it. As a result, organisations need to treat privacy as both a compliance and business risk issue, in order to reduce regulatory sanctions and commercial impacts.

3. Reputational damage

Attackers have become more organised, attacks have become more sophisticated, and all threats are more dangerous, and pose more risks, to an organisations reputation. With the speed and complexity of the threat landscape changing on a daily basis,



all too often we're seeing businesses being left behind, sometimes in the wake of reputational and financial damage. Organisations need to ensure they are fully prepared and engaged to deal with these ever-emerging challenges.

4. Privacy and regulation

Most governments have already created, or are in the process of creating, regulations that impose conditions on the safeguard and use of Personally Identifiable Information (PII), with penalties for organisations that fail to sufficiently protect it. As a result, organisations need to treat privacy as both a compliance and business risk issue to reduce regulatory sanctions and commercial impacts, such as reputational damage and loss of customers due to privacy breaches.



e *Most governments have already created, or are in the process of developing, regulations that impose conditions on the protection and use of PII.*

Different countries' regulations impose different requirements on whether PII can be transferred across borders. Some have no additional requirements; others have detailed requirements. In order to determine what cross-border transfers that will occur with a particular cloud-based system, an organisation needs to work with their cloud provider to determine where the information will be stored and processed.

5. Cybercrime

Cyberspace is an increasingly attractive hunting ground for criminals, activists and terrorists motivated to make money, get noticed, cause disruption or even bring down corporations and governments through online attacks.

Organisations must be prepared for the unpredictable, so they have the resilience to withstand unforeseen, high impact events. Cybercrime, along with the increase in online causes

(hacktivism), the increase in cost of compliance to deal with the uptick in regulatory requirements, coupled with the relentless advances in technology against a backdrop of under-investment in security departments, can all combine to cause the perfect threat.

Organisations that identify what the business relies on most will be well placed to quantify the business case to invest in resilience, therefore minimising the impact of the unforeseen.

6. The internet of things

Organisations' dependence on the internet and technology has continued to grow over the years. The rise of objects that connect themselves to the internet is releasing a surge of new opportunities for data gathering, predictive analytics and IT automation.

As increased interest in setting security standards for the internet of things (IoT) escalates, it should be up to the companies themselves to continue to build security through communication and interoperability. The security threats of the IoT are broad and potentially devastating and organisations must ensure that technology for both consumers and companies adheres to high standards of safety and security.

You cannot avoid every serious incident, and while many businesses are good at incident management, few have a mature, structured approach for analysing what went wrong. As a result, they are incurring unnecessary costs and accepting inappropriate risks.

By adopting a realistic, broad-based, collaborative approach to cyber security and resilience, government departments, regulators, senior business managers and information security professionals will be better able to understand the true nature of cyber threats and respond quickly, and appropriately. ■

Basic PC protection for technophobes

The Information Services and Technology Department (IST) of MIT offers these 10 safe computing tips:

PC protection for technophobes - the Information Services and Technology Department (IST) of the Massachusetts Institute of Technology (MIT) offers these 10 safe computing tips:

1. Patch, Patch, PATCH!

Set up your computer for automatic software and operating system updates. An unpatched machine is more likely to have software vulnerabilities that can be exploited.

2. Install protective software.

Free downloads such as Avast, AVG, MBAM are available for PCs. When installed, the software should be set to scan your files and update your virus definitions on a regular basis.

3. Choose strong passwords.

Choose strong passwords with letters, numbers, and special characters to create a mental image or an acronym that is easy for you to remember. Create a different password for each important account, and change passwords regularly.

4. Backup, Backup, BACKUP!

Backing up your machine regularly can protect you from the unexpected. Keep a few months' worth of backups and make sure the files can be retrieved if needed.

5. Control access to your machine.

Don't leave your computer in an unsecured area, or unattended and logged on, especially in public places. The physical security of your machine

is just as important as its technical security.

6. Use email and the internet safely.

Ignore unsolicited emails, and be wary of attachments, links and forms in emails that come from people you don't know, or which seem 'phishy.' Avoid untrustworthy (often free) downloads from freeware or shareware sites.

7. Use secure connections.

When connected to the Internet, your data can be vulnerable while in transit. Use remote connectivity and secure file transfer options.

8. Protect sensitive data.

Reduce the risk of identity theft.

Securely remove sensitive data files from your hard drive, which is also recommended when recycling or repurposing your computer. Use the encryption tools built into your operating system to protect sensitive files you need to retain.

9. Use desktop firewalls.

Macintosh and Windows computers have basic desktop firewalls as part of their operating systems. When set up properly, these firewalls protect your computer files from being scanned.

10. Most importantly, stay informed.

Stay current with the latest developments for Windows, Macintosh Linux, and Unix systems. ■





SECURITY SERVICES

The ISS Group was first established in 1901 as a Danish Security Company. Over the last century, ISS has developed into a leading provider of Facility Services employing over 500,000 people across more than 50 countries.

Locally, ISS Security has enjoyed a predominant position in the market for over 25 years. Today, our 3,500 employees are specialized in providing total security solutions for our clients.

ISS Security is dedicated to understanding clients' needs and exceeding their expectations.

Our Services:

- Security Guarding (Premium, Ex-Gurkha, Local and Armed)
- Design, Installation and Maintenance of Security Systems
- Central Station Alarm Monitoring
- Close Escort Service, X-ray Screening
- Security Consultancy, Event Planning and Operation
- Mobile Patrol
- Guard Dogs

Tel: (852) 2729 2266

Fax: (852) 3188 0879

Website: www.asf.com.hk

E-mail: asf.hotmail@hk.issworld.com

Address: 3/F United Overseas Plaza, 11 Lai Yip Road,
Kwun Tong Kowloon, Hong Kong

R&R PUBLISHING



R&R Publishing is a media and communications company based in Hong Kong specialising in custom publishing, design and production of a wide range of marketing materials, including:

- Custom Magazines
- Newsletters & Brochures
- On-line Publications
- Annual Reports
- Branding
- Marketing Materials
- Directories
- Websites

We focus on crafting individual solutions for companies and corporations in Hong Kong, around the region and internationally. Our high-quality services enable you to grow your business and reach out to your customers.

We link the creativity of our highly experienced editors, writers, designers and production staff with the latest technology to provide you with the tools you need to promote your brand, products and services to your customers and target audience.

Contact us now to see how we can help promote your business!



R&R Publishing Ltd

705, 7/F Cheong K. Building, 84-86 Des Voeux Road Central, Hong Kong
Tel: (852) 2126 7815 Email: info@rrpublishing.com.hk

www.RRPublishing.com.hk

New analogue cameras

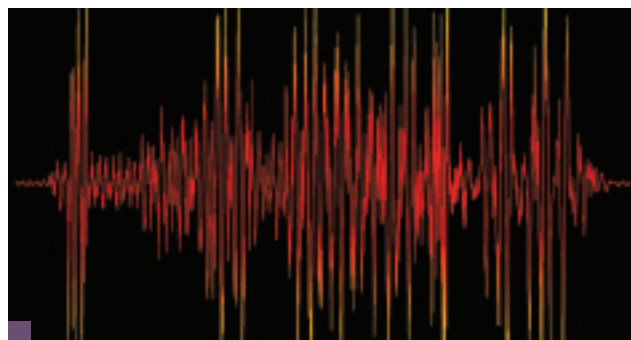
The **TeleEye Group** have introduced a new set of analogue surveillance cameras. Their range of 700 TV Lines (TVL) analogue cameras capture video in high resolution and are aimed at businesses that want to upgrade their existing coax infrastructure yet avoid the costs associated with switching to IP technology.

The Group also recently added an IR vari-focal dome camera: the MX925-HD, to its range of 1080p HD cameras. TeleEye claim the new camera is hacker-resistant and can save up to 50% network bandwidth compared to cameras using H.264 video codec.

The TeleEye Group recently announced the establishment of its 10th overseas office in Kuala Lumpur, Malaysia on 31st October 2013.

On the subject of Asia expansion, New Zealand-based integrated access control and perimeter protection company **Gallagher** is extending its reach to Thailand and surrounding countries following increasing demand from the Asian market. Gallagher's Bangkok office will be open and operational by the end of the year and the company is currently recruiting staff.

Closer to home, the company was a Silver Sponsor of the recent Asia-Pacific Security Forum & Exhibition in Macau and showcased its v7.10 Command Centre. The system resides on an organisation's IT network and integrates electronic access control, intruder alarms management, perimeter security and compliance management.



Malware in the Air

In a recent paper published in Journal of Communications Vol. 8 no. 11 entitled On Covert Acoustical Mesh Networks in Air, researchers Michael Hanspach and Michael Goetz describe how they constructed a covert channel between different computing systems separated by an air gap that utilised audio modulation/demodulation to exchange data between the computing systems. They go on to state “It is shown that the concept of a covert acoustical mesh network renders many conventional security concepts useless, as acoustical communications are usually not considered.”

In other words, an attacker could take advantage of the computer systems' speakers and microphones normally used for such activities as IP telephony and exchange information at inaudible frequencies. Aside from simply switching off the audio devices (which may not always be feasible), the authors suggest countermeasures such as audio filtering to prevent computers from participating in covert acoustical networks.

Do Not Track app for Android

Security software company AVG has added a 'Do Not Track' (DNT) feature to its free PrivacyFix app for Android mobile phones. Advertisers have moved on from collecting information on our browsing histories to tracking our physical locations. By doing this it is possible to collect more information on our habits and routines and streamline their advertising efforts.

PrivacyFix allows mobile users to discover who is tracking website visits and either block or allow it; the update will prevent Android phones from transmitting their MAC address or connecting to unapproved Wi-Fi networks — automatically suspending Wi-Fi connections to all but preselected trusted networks.

AVG's vice president of privacy products believes that tracking should be turned off until retailers adopt 'meaningful standards' of transparency and offer users clear choices of opting out of these programmes.

[illegible]

Millimetre waves see bombers at a distance

Sophisticated next-generation radar systems are being designed to detect would-be bombers at long distances, in crowded areas, and even at non-'fixed' locations.

Person-borne improvised explosive devices (PBIEDS) are often shaped from a variety of metals and concealed under clothing or in backpacks so they are extremely difficult to detect. The US-based ALERT (Awareness and Localisation of Explosives Related Threats) Center - a partnership of academic, industrial and government entities - is developing multiple radar units that can be pointed in the direction of crowds of people that are approaching a venue, checkpoint, or other area of entry.

The system would scan each individual at a distance of 50 metres or more to identify suicide bombers who appear to be dressed normally, but are concealing IEDs strapped to their bodies.

The ALERT Center's system uses a millimetre wave based design approach. Millimetre waves are a subset of the microwave band and operate within a frequency range of 30-300 Ghz. Unlike X-rays, millimetre-waves are non-ionising and universally considered non-carcinogenic.

The ALERT radar is expected to be mountable to a van or truck for wide-ranging field use. Permanently mounted solutions would also be available for high security buildings, checkpoints or border crossings.

Balloon power for disaster zones

Lasers and balloons may seem an unlikely mix, but Professor Stephen Blank of the New York Institute of Technology is working on an idea to send electrical power over long distances using powerful lasers and tethered aerostats. Aerostats are buoyant gas filled balloons widely used as surveillance platforms by the US military in such places as Afghanistan. Blank's idea is to send a laser signal up to a local aerostat through a fibre-optic cable, beam it through the air to a distant aerostat where the high-energy light would be converted into electricity and conducted back down to earth via the far aerostat's tether. In this way, hundreds of kilowatts of power could be transmitted over several hundred kilometres. Getting energy into disaster zones could be one of the first uses, says Blank, pointing to the aftermath of typhoon Haiyan in the Philippines. "You could have an aircraft carrier off the coast of the Philippines, with its nuclear generator, beaming power where it's needed."



AFSCO
ELECTRIC FENCES

The low-cost solution to high-cost crime

**Your house is worth millions. Your family is priceless.
Install an unobtrusive AFSCO electric fence – the
ultimate in perimeter protection.**



DEFEND... DETER... DENY... DETECT

Phone: 2880 0512

Email: afscok@sprintlocks.com

www.sprintlocks.com

NSA and GCHQ finger internet company fibres

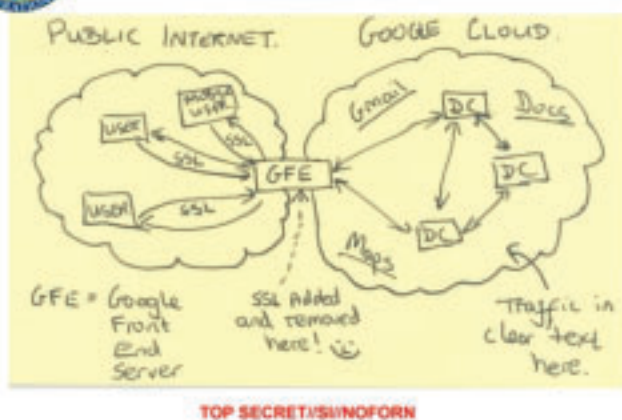
In a joint project codenamed MUSCULAR, the USA's National Security Agency and the UK's Government Communications Headquarters have been collecting data from the private fibre networks linking the data centres of Google and Yahoo, according to yet another Snowden leak and confirmed by unnamed sources.

Although data sent from a user to a Google or Yahoo internet account is encrypted, the internet companies store copies of that information on servers in data centres around the world. This reduces possible data loss in the event of failure. However, the private fibre links between data centres are not encrypted and it is here that MUSCULAR taps in to collect the data.

Both Google and Yahoo already comply with the NSA's PRISM which legally compels technology companies to submit data that matches certain court-approved search criteria and this additional secret access appears to have shocked the senior management of these internet giants. In a company statement, Google's chief legal officer David Drummond said "We are outraged at the lengths to which the government seems to have gone to intercept data from our private fibre networks."



Current Efforts - Google



Not a 'PostIt' but a Slide from a NSA presentation (Washington Post)

Zombie drones coming to a park near you

Inspired by Amazon's plan to use drones to deliver packages to customers, programmer Samy Kamkar wrote software he called SkyJack that controls a drone that flies around seeking out the Wi-Fi control signals of other drones. It then cuts their wireless connections and establishes itself as the controller – allowing people to make other drones do their bidding. The code is freely available on github.com and turns drones into 'zombies', says Kamkar.

The software runs on Linux machines (Kamar used a Raspberry Pi) and is effective on AR drones manufactured by French company Parrot. Would-be Skyjackers don't even need a drone of their own; a ground-based controller with a Linux laptop can create a zombie army from drones that fly into range.

New security cameras to detect violent motions

A special CCTV camera might know what you are doing, thanks to a monitoring system that can detect aggressive behaviour.

According to New Scientist, Kintense, which is based on Microsoft's, gaming sensor Kinect, analyses a person's body and picks out where the joints are to create a real-time 3D skeleton figure. An algorithm then recognises movements made by this model that indicate aggressive acts such as kicking, pushing, hitting and throwing.

Unlike Kinect, Kintense doesn't require people to be facing the camera. In trials, some actions like kicking were recognised with 90 per cent accuracy, but other movements, like punching and throwing, were trickier to spot. The system, designed by researchers at the University of Virginia, was created to warn medical staff if a patient is acting violently – but it could also be used in security cameras. It was presented at the SenSys conference in Rome, Italy.

"Using vision and acoustic sensors originally developed for games is now a very powerful paradigm for many different kinds of applications, including health," says team member Jack Stankovic. They plan to upgrade the system so it can recognise verbal aggression, too.



Now boarding – wine and beer

Los Alamos National Laboratory recently demonstrated a magnetic resonance imaging system called 'MagRay' that developers say is better than X-rays at differentiating bomb-making substances from benign substances. "A technique like magnetic resonance is very well suited for looking at liquids and gels," said MagRay project leader Michelle Espy.

According to Espy, the traditional carry-on baggage scanning method using X-rays misses certain threat indicators. What appears to be a bottle of white wine could be nitromethane, an ingredient for explosives. The new approach could rapidly and accurately discriminate between liquids that look identical.

The new system assesses proton content, MRI measurements and X-ray density data.

With a simple user interface, operators would insert a bottle into the machine and, without any calibrating, see a display consisting of "not much more than red light, green light - either this is bad or you can let this go," MagRay engineer Larry Schultz said.

Google Glass wearers get poke in eye

Negative reactions to Google Glass have been making headlines lately. In particular, restaurants, café and bars have shown an antipathy to Glass users. Wearers have been bemused to find themselves referred to rather rudely as 'Glassholes.'

"People make a personal decision to check their smartphone or log in and check their social media accounts, but Google Glass is out of their control," said Larry Rosen, a psychologist who focuses on technology. "They are not able to make a decision as to whether they want to be 'on' or 'connected' through someone else's process, and they are concerned and unhappy that they do not have a say in the matter."

People feel in control when using their own technology but, fairly or not, Google Glass seems to them more like invasive surveillance. One of the primary concerns people have about Glass is that it is difficult to tell when the device is recording you. With a phone, a stranger would have to physically hold up the device and point the camera in the subject's direction, a visible cue that they are recording. Wearable cameras like Glass are always pointed and ready to go.

An organisation called 'Stop the Cyborgs' has been founded in response to the combination of wearable technology with 'big data.' On their website, they state "Stop the Cyborgs is not anti-Glass; we just want to proactively shape the norms around its use. The issue is simple politeness."



Emphasis on stinky terrorists

Terrorists constructing home-made bombs in suburban premises may be caught out by sensors in the sewer system under a European Union-funded research programme called Emphasis.

The approach centres on the fact that gases and liquids from bomb production (or for that matter, illicit drug production) enter the air and sewers through windows, skylights, baths, sinks and toilets. An example of this occurred at the house used to prepare explosives for the London bombings of July 2005 in which 54 people died – the fumes killed off many of the plants in the garden.

As bomb-making chemicals break down, specific ions are released which can be detected by a network of sensors. The sensors consist of several 10cm long ion-selective electrodes which are submerged in the wastewater flowing through the sewer system. Above ground, static sensors monitor the air over distances up to 400m for explosives present in the vapour stage.

Once a command centre processes the data sent from the sensors and a positive detection is made, a covert mobile detection team would move in to pinpoint the bomb factory location.

The system is currently undergoing testing under laboratory conditions and will be tried out in actual sewers in the coming year. The sensors could also be used for real-time monitoring of illicit drug use and detection of illegal drug factories.

A Roman Holiday?

BRING 24-HOUR SECURITY

“...the Camorra makes the Sicilian Mafia look like the Salvation Army.”

By Peter Sherwood

The glory that was Rome (emphasis on was) today lies mangled under the horrors of millions of tourists in summer alone. Seeing stylish Italy has always been a balance between a rich cultural heritage and being hustled.

Gibbon's masterpiece 'The Decline and Fall of the Roman Empire' is centuries old, but to plot more recent deterioration in things Italian try the reptilian crook Silvio Berlusconi, elected three times to its highest office. (Since World War Two the country has had more governments than Julius Caesar had dagger wounds).

Lovely people the Italians, but decay and security concerns begin at Rome's airport and continue to Termini train station, a joint venture between Robert Mugabe's Zanu PF party the Afghan Jockey Club. No map of the Italian rail system exists at this shambolic enterprise where information officers greet you like the Black Death. And nobody knows less about railway schedules than the bleak lady at the end of a 45-minute ticket queue whose daily joy is praying you've missed your train.

At airport immigration half a dozen yawning blokes rummage through their trousers for something interesting to scratch, while passengers wait... and wait. The baggage equipment was high tech in Mussolini's day and is operated by workers suffering narcolepsy,

while pilfering remains a traditional art form (recently police arrested 19 baggage handlers at the airport as part of a probe into widespread suitcase looting).

Nail your stuff to your chest or you'll get something pinched, as I discovered later in Naples. What I was doing in that festering, gangster-run dump defies rational explanation: the Camorra makes the Sicilian Mafia look like the Salvation Army. Pickpockets swarmed. I found myself on a packed bus going "Uh, oh!" as, almost immediately, greedy hands slid into every pocket. The bloke thrust up against me was part of scam. Bravely I pushed my free arm against his throat and pointed my fingers at his eyes like the Three Stooges. I say 'bravely' meaning stupidly; a sharp object could have ripped my heart out and nobody would notice until the mob dispersed and I fell flat on my face. Happily, all I lost was a camera.

I didn't know what might be more depressing; staying in Rome forever or a reprise of the airport fiasco, which on any given day is like the apocalypse in



slow motion. Entering the departures terminal (words suggesting you might simply give up and end it all) I was met by a sweating mass of humanity on its hour-long crawl to a couple of tired security machines operated by what appeared to be the Italian Gestapo. Quietly, I joined them, suppressing an urge to strangle someone. ■

Peter Sherwood is a long-term Hong Kong resident. For eight years he wrote a regular satirical column for the SCMP. He is the author of 15 books.

Security Asia magazine can help grow your business!

It's a bold claim – so how can we help you? Here's how:

- We'll keep you informed of the latest developments and trends in the security industry with feature articles written by experts.
- We present new and interesting products with our regular 'Latest Security Devices' article.
- If your company has a unique product or service, tell us about it and we may showcase it in an editorial.
- Security Asia is read by over 10,000 professional people directly related to the security industry. It is mailed to senior executives and decision-makers who choose to purchase products and services.
- We can work together to promote your business to exactly the right people.
- No other local magazine gives you access to the region's security elite.

**Call Colin on (852) 2126 7812,
email Advertising@RRPublishing.com.hk
or visit our web page
www.Security-Asia.net/advertise-with-us
to find out how we can help grow your business.**

**For more information about *Security Asia*, please
visit our website, www.Security-Asia.net**



SecurityAsia is delivered directly to associations and decision makers who are responsible for purchasing security related services and products including:

- Members of The HKSA
- Government security bureaus
- Security consultants
- Law and accountancy firms
- Financial institutions
- Insurance companies
- Transportation companies
- Facilities management providers
- Security hardware and software manufacturers



Security Asia is the only magazine published in Hong Kong for the security industry and endorsed by The Hong Kong Security Association. It is distributed throughout the Asia-Pacific region.

R&R
PUBLISHING

R&R Publishing Ltd

705, 7/F, Cheong K. Building, 84-86 Des Voeux Road Central, Hong Kong
Tel: (852) 2126 7814 Email: Advertising@RRPublishing.com.hk
Web: RRPublishing.com.hk

The ASA Group

S e c u r i t y & A v i a t i o n



**Specialist providers of
trustworthy private
aviation and VIP security
services throughout the
Asia Pacific region**



- **Full Ground Handling, Supervisory and Coordination Services**
- **Landing & Overflight Permits**
- **Private Charter Flights**
- **Secure Transportation for Crew and Passengers**
- **VIP Executive Protection and Security Services**

For more information, please call Joe Wilson on +852 9866 6764

Email: enquire@asag.aero

Website: www.asag.aero

Hong Kong | Macau | China | Taiwan | Thailand | Cambodia | Laos | Vietnam
Myanmar | Singapore | Malaysia | Indonesia | Philippines | South Korea | Japan