KEEP CALM and Carry On: PRISM itself is not a big deal

But yes, Skype's no longer safe ... and keep an eye on GCHQ

By Duncan Campbell, 11th June 2013

RELATED STORIES

- REVEALED: The gizmo leaker Snowden used to smuggle out NSA files
- CRINGE! Home Office wants to know whether your boss BEATS YOU
- Japan proposes NSA-style agency and new snooping laws
- PRISM snitch claims NSA hacked Chinese targets since 2009
- NSA: 'Dozens of attacks' prevented by snooping

http://www.theregister.co.uk/2013/06/11/prism_numbers_not_adding_up/

- Prism
- National Security Agency
- Cia
- Eavesdropping
- Edward Snowden

Analysis PRISM, the top secret US National Security Agency web communications and user data collection program revealed by whistleblower Edward Snowden last Friday, and targeted on nine top US web service providers, would seem unlikely to be the total, tyrannical surveillance behemoth reporters first assumed.

That's because its numbers, as published, just don't add up.

The Guardian may also have missed a potentially significant scoop buried within the PRISM revelations – apparent confirmation that about the time in 2011 that Microsoft acquired Skype for $7bn, the U.S. government also acquired a back way in to the previously secure, complex and highly trusted peer-to-peer voice over IP system.

Analysis also suggests that the much more complex surveillance system that the Home Office wants installed in Britain using powers proposed in the now discredited draft Communications Data Bill (CDB) would be far more intrusive than PRISM.

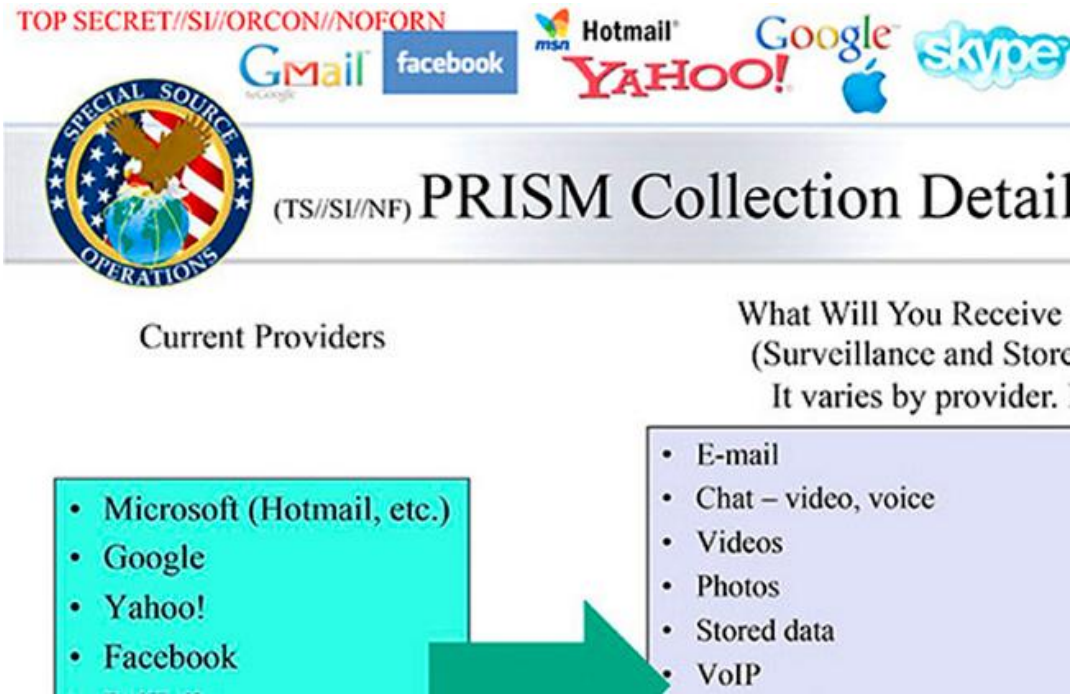
PRISM intelligence collection, despite the hullabaloo, is phrased in terms of "requests" to be made to specified US service providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. While the slides published by *The Guardian* do refer to "collection directly from the servers of these [companies]", this appears to refer to links from NSA central systems to special company servers facilitating law enforcement or intelligence data queries, not to huge pipes into entire petabyte scale company databases.

The NSA has numerous other collection programs, including deep packet inspection (DPI) systems akin to those sought in the CDB. Some were planned in the late 1990s. These include the secret room installed in AT&T's internet exchange and peering point in downtown San Francisco and revealed by whistleblower Mark Klein in 2006. The San Fran secret room was fed by optical fibres spliced into most of the US west coast Internet backbone. These fed into high end DPI analysis equipment, whose output was presumed to be routed back to NSA.

The NSA also has access to global communications satellite traffic through a series of programmes and ground stations starting with ECHELON in 1968, and to global submarine cable traffic through interception points located at or near cable landing sites in the US, UK and other

co-operating countries. A specially equipped nuclear submarine, the USS *Jimmy Carter*, carries cutting, tapping and interception systems to lie on the sea bed. The submarine has been in active service since 2005.

According to the “overview” slide, PRISM is “the SIGAD [Sigint Activity Designator] used most in NSA reporting” (emphasis in original). The PRISM collection program was also designated US-984XN, and is run by NSA’s “special source operations” office, whose logo sports a globe ensnared and held in the talons of the US eagle.



Top Secret, Special Intelligence, No Foreigners ... well, except GCHQ probably

PRISM’s own widely displayed logo, a prism dispersing light into a spectrum, has been inferred by commentators to point to the separation of light carriers in optical transmission systems, and thus to hint at PRISM being associated with fibre level interception of Microsoft and other companies’ traffic. But this makes little sense, as immense cryptologic and analytic resources would have to be deployed at interception centres to decrypt and analyse SSL and other layers and to assemble messages from packets carried over divergent routes. They would cost much but deliver little actionable intelligence.

The better interpretation may be more banal. NSA’s codeword central office handed out the latest available batch of codewords, PRISM was selected, and a pretty logo designed to match.

PRISM’s reported costs are so small, it has to be mighty simple.

According to the 41 slide classified PRISM powerpoint prepared for NSA trainees and published by *The Guardian*, PRISM costs about $20m dollars a year. During 2012, the slides say, 24,005 NSA Sigint reports cited PRISM as a main source. The total number of such reports since the program started in 2007 is said to be 77,000.

Heavy duty sigint surveillance contractors – and the US has hundreds of them collecting and sifting the world’s communications – wouldn’t get out of bed for less than $100m. Want a decent collection system, a few bases, lots of custom signal processors, perhaps a space segment? You're talking $$ billions. NSA’s overall budget is classified, but even excluding dedicated military services it is estimated to be more than $10bn.

In the world of global sigint, $20m is small change. The average cost of each PRISM derived report in 2012 would be $830. This average amount could be little more than agreed payments on agreed scales for the US companies to hand over agreed types of information in response to law enforcement requests, plus a contribution to maintaining specialised interface facilities.

More significantly, PRISM's numbers are far smaller than some of the companies involved have already disclosed when revealing the number of US law enforcement or government disclosure requests they handle and pass through each year.

Microsoft says that during 2012, they processed 70,665 law enforcement and other government requests for information, mainly for United States agencies. They also admitted disclosing the content of Hotmail and other communications to law enforcement agencies in the United States in 1,544 cases.

Content usually *isn't* king, when you're a spook

Most of these requests were for what Microsoft calls "noncontent data", such as account holders' names and addresses, gender, e-mail addresses, IP addresses used, and dates and times of message or data transmissions, while 2 per cent of the requests were for the contents of e-mails or of files stored on SkyDrive.

Where did the guys who did the Olympics 2012 logo go next?

Skype, owned by Microsoft, has admitted disclosing administrative details of 4,713 Skype accounts during 2012, including Skype user IDs, supplied names, e-mail address and billing information, as well as call detail records if a person subscribes to Skype In or Skype Out services that connect to the normal telephone network.

According to the *New York Times*, Microsoft released no content from Skype transmissions during 2012, allegedly because "the peer-to-peer nature of Skype's Internet conversations means the company does not store and has no access to past conversations."

This and more recent and carefully worded statements from Microsoft fail to deny that if a Skype ID is targeted for interception, VOIP call content can then be copied to an interception centre and recorded.

But Microsoft's statement is irrelevant because precisely the same situation applies as for normal telephony; there is no automatic recording of calls, so past conversations that were not intercepted at the time can never be accessed. But once an electronic tap is in place, everything can be rerouted, monitored and stored by the requesting agency. Many privacy activists suspect

that when Microsoft re-engineered Skype supernodes to be exclusively under company control in 2012, the interception gateways were opened up.

Google's 2012 transparency report says that it received and processed 47,479 US law enforcement requests for information – about double the total number of NSA PRISM reports produced in the same year.

All nine US companies are reported to have stated they had never heard of PRISM before *The Guardian* report came out. From material published to date, there is no reason to disbelieve this, as PRISM appears to be no more than the internal, secret NSA name for intelligence sources that provide an internal web page to authorised analysts, from which users can choose from a shopping list of which company to go to and what each company has agreed to supply. Why should the companies have known the secret internal name?

What all of them have done, and some like Google and Microsoft been moderately open about describing in disclosure statements and pages, is to set up offices and rooms and systems which service authorised law enforcement (including intelligence agency) requests, and have them extracted from their record base by bespoke systems.

This is very different from wholesale access, downloading, and general trawling and data mining. *The Guardian* scoop the day before PRISM revealed a secret warrant directed to communications provider Verizon requiring wholesale delivery of all call data records from their entire system. That, and doubtless a flood of identical orders to other communications companies, is unambiguous data mining and warrantless surveillance.

PRISM thus also appears little different from what goes on in over a hundred SPOC (Single Point of Contact) offices in UK police and other agencies, where specially trained officers receive signed authorities under the 2000 Regulation of Investigatory Powers Act (RIPA) to go collect communications data. All major UK telcos now provide secure web interfaces through which SPOCs can give their IDs and passwords, insert the authorised requests and then receive web or e-mail downloads of the requested data.

In contrast to the US, no UK CSP or telco publishes figures as to the number or type of law enforcement or intelligence agency requests they receive. They are not permitted to reject requests, US companies can inspect the requests and say no – and tell the public how much is asked, and how much rejected.

PRISM appears only to differ from what is now in place for both US and UK telcos in that it accesses web based services. Britain has no equivalent companies, as they are all US based, so and requests would have to be routed there.

The Guardian has quoted a figure of 187 requests processed by NSA for GCHQ during 2012. This too is a small number. GCHQ's requests could easily be compliant with British law, provided that normal RIPA requests were made, and then passed to GCHQ analysts with online access to NSA's PRISM page.

Significantly, when GCHQ recently gave evidence to the Intelligence and Security Committee in support of the Communications Data Bill, they may have forgotten to mention that they already had access to Hotmail and Gmail and many of the other services which they said were "black holes" requiring new systems and powers. We do not know for sure, as some of their evidence was redacted. It will have to be checked again by those in the know.

Ironically, the PRISM disclosure may, when more carefully considered, buttress the continuing British campaign against the re-introduction of the CDB – not because PRISM surveillance was unlawful, but because, being lawful, it shows that GCHQ and the Home Office were having Parliament on when they demanded new powers and systems for Internet intrusion.

The picture of PRISM that emerges from this analysis leaves me uncomfortably comfortable with the claims made by Barack Obama and William Hague alike: that PRISM complies with applicable law, and may be stature or warrant based - and need not be disproportionate, despite the alarm engendered by NSA's boasting.

The opposite is the case with the wholesale copying of call data records from Verizon and, in all probability, from other US carriers. Whether the same happens between GCHQ and O2, EE, Vodafone, BT and Three is not known.

The bottom line on PRISM in particular may be that NSA doesn't just bug us big time, all the time. They also do braggadocio, big time. ®

Duncan Campbell trained in physics and has worked as an investigative journalist and television reporter and producer since 1975, specializing in investigating sensitive political topics, including defense, policing, intelligence services and electronic surveillance. His scoops include revealing many aspects of international espionage, including telephone tapping and the Echelon satellite interception network.

Lies, Damned Lies and Guesswork

I'll counter-guess: Those 20 millions are solely for requesting crypto keys from Skype. Google and Facebook. When they have that, the already-in-place Collection System will do the rest.

There is only a single secure approach: Get Out Of The Cloud Now !

+ TOR always, early and often erasing of cache

+ Raspberrry PI hosting your files

+ GNUpg encrypting messages

+ TrueCrypt encrypting your files

+ Cola bottles in the woods storing your encrypted backup memory sticks

+ encrypted chat over your own chat server running on the RaspPI

+ Raspberry PI server runs your email server

Essentially, boycott the business of Brin, Zuckerberg and Ballmer. Those are 100% subverted by an security services running amok.

---

http://www.duncancampbell.org/menu/surveillance/echelon/IC2000_Report%20.pdf

http://www.duncancampbell.org/menu/journalism/newstatesman/newstatesman-1988/They%27ve%20got%20it%20taped.pdf

http://www.duncancampbell.org/

http://www.duncancampbell.org/content/echelon

http://www.nsawatch.org/echelon.html

http://www.ncoic.com/nsapoole.htm

EPIC Report
Duncan's report for the Electronic Privacy Information Center [EPIC], based in Washington DC which investigated the US National Security Agency's use of surveillance and it's effect on human rights.
Click here to read more

ICIE2001:Echelon and its role in COMINT
Paper 1 of Duncan's 'Interception Capabilities: Impact & exploitation 2001' clarifies many of the misconceptions and misreporting of Echelon.
Click here to read more

ICIE2001: COMINT Impact on international trade
Using detailed, entirely American original sources, 'Paper 2' argues the significant economic and employment losses caused by Echelon's misuse.
Click here to read more

ICIE2001: COMINT, privacy and human rights:
'Paper 2' reveals the extent to which Echelon and Communications intelligence is purposed towards the protection of US interests over European ones.
Click her to read more

EU Parliament Resolution
The full European Parliament resolution on Echelon.
Click here to read more

Ex-CIA director on Echelon
Former-CIA director James Whoolsey remarks on Echelon at the foreign press centre in Washington DC in 2000.
Click here to read more

Chronology
A timeline of the changes in Echelon's history, going back to 1964.
Click here to read more

"Success stories"
A list of cases where Echelon was used for industrial espionage purposes.
Click here to read more

The Wall Street Journal, March 17, 2000 http://cryptome.org/echelon-cia2.htm

Why We Spy on Our Allies

By R. James Woolsey, a Washington lawyer and a former Director of Central Intelligence.

What is the recent flap regarding Echelon and U.S. spying on European industries all about? We'll begin with some candor from the American side. Yes, my continental European friends, we have spied on you. And it's true that we use computers to sort through data by using keywords. Have you stopped to ask yourselves what we're looking for?

The European Parliament's recent report on Echelon, written by British journalist Duncan Campbell, has sparked angry accusations from continental Europe that U.S. intelligence is stealing advanced technology from European companies so that we can -- get this -- give it to American companies and help them compete. My European friends, get real. True, in a handful of areas European technology surpasses American, but, to say this as gently as I can, the number of such areas is very, very, very small. Most European technology just isn't worth our stealing.

Why, then, have we spied on you? The answer is quite apparent from the Campbell report -- in the discussion of the only two cases in which European companies have allegedly been targets of American secret intelligence collection. Of Thomson-CSF, the report says: "The company was alleged to have bribed members of the Brazilian government selection panel."

Of Airbus, it says that we found that "Airbus agents were offering bribes to a Saudi official." These facts are inevitably left out of European press reports.

That's right, my continental friends, we have spied on you because you bribe. Your companies' products are often more costly, less technically advanced or both, than your American competitors'. As a result you bribe a lot. So complicit are your governments that in several European countries bribes still are tax-deductible.

When we have caught you at it, you might be interested, we haven't said a word to the U.S. companies in the competition. Instead we go to the government you're bribing and tell its officials that we don't take kindly to such corruption. They often respond by giving the most meritorious bid (sometimes American, sometimes not) all or part of the contract. This upsets you, and sometimes creates recriminations between your bribers and the other country's bribees, and this occasionally becomes a public scandal. We love it.

Why do you bribe? It's not because your companies are inherently more corrupt. Nor is it because you are inherently less talented at technology. It is because your economic patron saint is still Jean Baptiste Colbert, whereas ours is Adam Smith. In spite of a few recent reforms, your governments largely still dominate your economies, so you have much greater difficulty than we in innovating, encouraging labor mobility, reducing costs, attracting capital to fast-moving young businesses and adapting quickly to changing economic circumstances. You'd rather not go through the hassle of moving toward less *dirigisme*. It's so much easier to keep paying bribes.

The Central Intelligence Agency collects other economic intelligence, but the vast majority of it is not stolen secrets. The Aspin-Brown Commission four years ago found that about 95% of U.S. economic intelligence comes from open sources.

The Campbell report describes a sinister-sounding U.S. meeting in Washington where -- shudder! -- CIA personnel are present and the participants -- brace yourself -- "identify major contracts open for bid" in Indonesia. Mr. Campbell, I suppose, imagines something like this: A crafty CIA spy steals stealthily out of a safe house, changes disguises, checks to make sure he's not under surveillance, coordinates with a spy satellite and . . . buys an Indonesian newspaper. If you Europeans really think we go to such absurd lengths to obtain publicly available information, why don't you just laugh at us instead of getting in high dudgeon?

What are the economic secrets, in addition to bribery attempts, that we have conducted espionage to obtain? One example is some companies' efforts to conceal the transfer of dual-use technology. We follow sales of supercomputers and certain chemicals closely, because they can be used not only for commercial purposes but for the production of weapons of mass destruction. Another is economic activity in countries subject to sanctions -- Serbian banking, Iraqi oil smuggling.

But do we collect or even sort secret intelligence for the benefit of specific American companies? Even Mr. Campbell admits that we don't, although he can't bring himself to say so except with a double negative: "In general this is not incorrect." The Aspin-Brown Commission was more explicit: "U.S. Intelligence Agencies are not tasked to engage in 'industrial espionage' -- i.e. obtaining trade secrets for the benefit of a U.S. company or companies."

The French government is forming a commission to look into all this. I hope the commissioners come to Washington. We should organize two seminars for them. One would cover our Foreign Corrupt Practices Act, and how we use it, quite effectively, to discourage U.S. companies from bribing foreign governments. A second would cover why Adam Smith is a better guide than Colbert for 21st-century economies. Then we could move on to industrial espionage, and our visitors could explain, if they can keep straight faces, that they don't engage in it. Will the next commission pursue the issue of rude American maitre d's?

Get serious, Europeans. Stop blaming us and reform your own statist economic policies. Then your companies can become more efficient and innovative, and they won't need to resort to bribery to compete.

And then we won't need to spy on you.

---

http://www.newstatesman.com/books/2010/06/gchq-agency-britain

---

China spy scare: hypocrisy is spelled Echelon

Or, why allies spy on each other

22 Feb 2010 19:06 | by John W. Daly in Münster | Filed in Security Google China

China has been receiving flak ever since Google confessed evil doers had cracked and compromised its systems, reading emails of Chinese dissidents. A steady stream of news has been gushing forth ever since, quoting diverse security experts and creating a sense of fear in regards to the yellow danger which is upon us, threatening our technological edge and the wealth it has bestowed upon us. Google even took up negotiations with the NSA, so None Such Agency may help ward off Dr. Fu-Manchu's sinister attacks on freedom and democracy.

However, the entire discussion is utterly hypocritical. Western allies have been spying on each other for decades, trying to oust each others rivalling industrial complexes and corporations from bids and steal patented technologies.

Back in 1993 and 1994, the German press had a field day after sources revealed French intelligence agency DGSE had intercepted a fax German conglomerate Siemens had sent to the South Korean government, containing an offer for a high-speed train system based on the German ICE. Apparently, the bid was shown to French train-maker GEC Alstom, whose Train de Grand Vitesse (TGV) was competing with Siemens. Despite widespread media coverage, both Siemens and the German government refrained from officially telling off France and resorted to making use of the silent channels of diplomacy.

Lack of evidence apparently was the main reason why senior management hushed the whole matter up. As a matter of fact, Siemens' CEO Heinrich von Pierer was rather upset when group executive manager Wolfram Martinsen lashed out accusations in an official protest note to the Korean government. Martinsen's memo was regarded as counterproductive as there was no sufficient evidence. Talks between GEC Alstom,

Siemens and the German Department of Transport were abandoned by the French. Nonetheless, the case is nearly always mentioned in hand-outs German students receive in internet security courses.

A couple of years later, English journalist Duncan Campbell reported to the European Parliament on the matter of Echelon, a vast eavesdropping network maintained by the NSA and the UK's very own GCHQ. Gathering economic intelligence became a main, yet unofficial directive in the early 1990ies, for members of the so-called UKUSA alliance. Echelon became a matter of parliamentary debate on the European level, especially after the Green faction decided there was enough evidence to support an official inquiry and added pressure.

Campbell wrote an article on Echelon back in 1998 for the New Statesman. As a delegate for the EU, Campbell penned a report entitled "Development Of Surveillance Technology And Risk Of Abuse Of Economic Information (An appraisal of technologies for political control)" for the EU Directorate General for Research.

The report cited an article from The Baltimore Sun, which stated the NSA had eavesdropped on satellite communications between Airbus and Saudi government officials concerning a deal with Saudi Airlines. Apparently Airbus officials wanted to bribe Saudi delegates - Boeing and McDonnell Douglas went on to win the $6 billion bid.

In March 2000, R. James Woolsey, a former Director of Central Intelligence, rebutted Europe's fears and public outcry concerning Echelon in an article for the Wall Street Journal. Woolsey stated in his commentary, aptly titled "Why we spy on our allies" that the US of A need not spy on European high-tech as US companies had the leading edge anyway. Instead the NSA spied on it's allies because European companies had to resort to tax-deductible bribery in order to win large contracts.

Mr Woolsey apparently forgot the Enercon case German newspaper Die Zeit reported on back in 1999. Enercon, a major German producer of wind turbines, received a written injunction in 1995 from a district court in San José and from the US Department of Commerce, claiming Enercon had infringed patents of Kenetech Windpower Inc.

Enercon's CEO Aloys Wobben had to appear in Washington and was questioned for two weeks. Wobbens's lawyers were able to view Kenetech Windpower's evidence - which included a detailed report on how Kenetech employees allegedly climbed up an Enercon E-40 turbine in 1994 and documented its inner workings over the course of an hour.

Apparently, the trio was able to access the turbine itself by disabling the security system. A journalist went on to tell Mr Wobben the NSA had previously intercepted security codes from Enercon and handed them over to Kenetech Windpower. Kenetech then sent it's engineers out to spy and patent a competitor's technology.

To cut a long story short - competitive intelligence is commonplace and has a long and very dirty history. All Western allies have been spying on one another for decades, even for centuries. France has been spying on Germany which has been spying around in the Balkan which was spied upon by the USA. Russia and China have been spying on the West since the 1990s, in an effort to modernise

their defunct industries. Get a life, move on, it is all old news.

Why then, may one beg, is there such an outrage about China?

The answer is simple: so "we" can openly shame China and influence public opinion on the newest member The Great Game's current edition. So the people in the West can feel ideologically superior to China. So McAfee, Booz Allen Hamilton and the likes can sell more and more services. To pit "us" against "them". There are a ton of reasons, yet none of them are actually worth the public outrage.

Just remember to fear US ambitions in terms of laying hands on banking data of EU citizens and companies as much as you now fear the Chinese intern.

Read more: http://news.techeye.net/security/china-spy-scare-hypocrisy-is-spelled-echelon#ixzz2WMJszr00

EUROPEAN PARLIAMENT

1999		2004

Session document

FINAL

A5-0264/2001

13. Conclusions and recommendations 'ECHELON'

13.1. Conclusions

The existence of a global system for intercepting private and commercial communications (the ECHELON interception system)

That a global system for intercepting communications exists, operating by means of cooperation proportionate to their capabilities among the USA, the UK, Canada, Australia and New Zealand under the UKUSA Agreement, is no longer in doubt. It may be assumed, in view of the evidence and the consistent pattern of statements from a very wide range of individuals and organisations, including American sources, that the system or parts of it were, at least for some time, code-named ECHELON. What is important is that its purpose is to intercept private and commercial communications, and not military communications.

Analysis has revealed that the technical capabilities of the system are probably not nearly as extensive as some sections of the media had assumed. Nevertheless, it is worrying that many senior Community figures, in particular European Commissioners, who gave evidence to the Temporary Committee, claimed to be unaware of this phenomenon.

The limits of the interception system

The surveillance system depends, in particular, upon worldwide interception of satellite communications. However, in areas characterised by a high volume of traffic only a very small proportion of those communications are transmitted by satellite. This means that the majority of communications cannot be intercepted by earth stations, but only by tapping cables and intercepting radio signals. However, inquiries have shown that the UKUSA states have access to only a very limited proportion of cable and radio communications, and, owing to the large numbers of personnel required, can analyse only an even smaller proportion of those communications. However extensive the resources and capabilities for the interception of communications may be, the extremely high volume of traffic makes exhaustive, detailed monitoring of all communications impossible in practice.

The possible existence of other interception systems

Since intercepting communications is a method of spying commonly employed by intelligence services, other states might also operate similar systems, provided that they have the required funds and the right locations. France, thanks to its overseas territories, is the only EU Member State which is geographically and technically capable of operating a global interception system by itself. There is ample evidence that Russia also operates such a system.

Compatibility with EU law

As regards the question of the compatibility of a system of the ECHELON type with EU law, it is necessary to distinguish between two scenarios. If a system is used purely for intelligence purposes, there is no violation of EU law, since operations in the interests of state security are not subject to the EC Treaty, but would fall under Title V of the Treaty on European Union (CFSP), although at present that title lays down no provisions on the subject, so no criteria are available. If, on the other hand, the system is misused for the purposes of gathering competitive intelligence, such action is at odds with the Member States' duty of loyalty and with the concept of a common market based on free competition. If a Member State participates in such a system, it violates EC law.

At its meeting of 30 March 2000 the Council made clear that it cannot agree to the creation or existence of an interception system which does not comply with the rules laid down in the laws of the Member States and which breaches the fundamental principles designed to safeguard human dignity.

Compatibility with the fundamental right to respect for private life (Article 8 of the ECHR)

Any interception of communications represents serious interference with an individual's exercise of the right to privacy. Article 8 of the ECHR, which guarantees respect for private life, permits interference with the exercise of that right only in the interests of national security, in so far as this is in accordance with domestic law and the provisions in question

are generally accessible and lay down under what circumstances, and subject to what conditions, the state may undertake such interference. Interference must be proportionate: thus competing interests need to be weighed up and it is not enough that the interference should merely be useful or desirable.

An intelligence system which intercepted communications permanently and at random would be in violation of the principle of proportionality and would therefore not be compatible with the ECHR. It would also constitute a violation of the ECHR if the rules governing the surveillance of communications lacked a legal basis, if the rules were not generally accessible or if they were so formulated that their implications for the individual were unforeseeable. Since most of the rules governing the activities of US intelligence services abroad are classified, compliance with the principle of proportionality is at least doubtful and breaches of the principles of accessibility and foreseeability laid down by the European Court of Human Rights probably occur. Although the USA is not itself an ECHR contracting party, the Member States must nevertheless act in a manner consistent with the ECHR. The Member States cannot circumvent the requirements imposed on them by the ECHR by allowing other countries' intelligence services, which are subject to less stringent legal provisions, to work on their territory, since otherwise the principle of legality, with its twin components of accessibility and foreseeability, would become a dead letter and the case law of the European Court of Human Rights would be deprived of its substance.

In addition, the lawful operations of intelligence services are consistent with fundamental rights only if adequate arrangements exist for monitoring them, in order to counterbalance the risks inherent in secret activities performed by a part of the administrative apparatus. As the European Court of Human Rights has expressly stressed the importance of an efficient system for monitoring intelligence operations, there are grounds for concern in the fact that some Member States do not have parliamentary monitoring bodies of their own responsible for scrutinising the secret services.

Are EU citizens adequately protected against intelligence services?

As the protection enjoyed by EU citizens depends on the legal situation in the individual Member States, which varies very substantially, and since in some cases parliamentary monitoring bodies do not even exist, the degree of protection can hardly be said to be adequate. It is in the fundamental interests of European citizens that their national parliaments should have a specific, formally structured monitoring committee responsible for supervising and scrutinising the activities of the intelligence services. But even where monitoring bodies do exist, there is a strong temptation for them to concentrate more on the activities of domestic intelligence services, rather than those of foreign intelligence services, since as a rule it is only the former which affect their own citizens.

In the event of cooperation between intelligence services under the CFSP and between the security authorities in the spheres of justice and home affairs, the institutions must introduce adequate measures to protect European citizens.

Industrial espionage

Part of the remit of foreign intelligence services is to gather economic data, such as details of developments in individual sectors of the economy, trends on commodity markets, compliance with economic embargoes, observance of rules on supplying dual-use goods, etc.

For these reasons, the firms concerned are often subject to surveillance. The US intelligence services do not merely gather general economic intelligence, but also intercept communications between firms, particularly where contracts are being awarded, and they justify this on the grounds of combating attempted bribery. Detailed interception poses the risk that information may be used as competitive intelligence, rather than combating corruption, even though the US and the United Kingdom state that they do not do so. However, the role of the Advocacy Center of the US Department of Commerce is still not totally clear and talks arranged with the Center with a view to clarifying the matter were cancelled. It should also be pointed out that an agreement on combating the bribery of officials, under which bribery is criminalised at international level, was adopted by the OECD in 1997, and this provides a further reason why individual cases of bribery cannot justify the interception of communications. At all events, it must be made clear that the situation becomes intolerable when intelligence services allow themselves to be used for purposes of gathering competitive intelligence by spying on foreign firms with the aim of securing a competitive advantage for firms in the home country. Although it is frequently maintained that the global interception system considered in this report has been used in this way, no such case has been substantiated.

The fact is that sensitive commercial data are mostly kept inside individual firms, so that competitive intelligence-gathering primarily involves efforts to obtain information through members of staff or through people planted in the firm for this purpose or else, more and more frequently, by hacking into internal computer networks. Only if sensitive data are transmitted externally by cable or radio (satellite) can a communications surveillance system be used for competitive intelligence-gathering. This applies systematically in the following three cases:

- in the case of firms which operate in three time zones, so that interim results are sent from Europe to America and on to Asia;

- in the case of videoconferencing within multinationals using VSAT or cable;

- if vital contracts are being negotiated on the spot (e.g. for the building of plants, the development of telecommunications infrastructure, the creation of new transport systems, etc.) and it is necessary to consult the company's head office.

Risk and security awareness in small and medium-sized firms is unfortunately often inadequate and the dangers of economic espionage and the interception of communications are often not recognised.

Since security awareness is likewise not always well developed in the European institutions (with the exception of the European Central Bank, the Council Directorate-General for External Relations and the Commission Directorate-General for External Relations), immediate action is therefore necessary.

Possible self-protection measures

Firms must secure the whole working environment and protect all communications channels which are used to send sensitive information. Sufficiently secure encryption systems exist at affordable prices on the European market. Private individuals should also be urged to encrypt e-mails: an unencrypted e-mail message is like a letter without an envelope. Relatively user-

friendly systems exist on the Internet which are even made available for private use free of charge.

Cooperation among intelligence services within the EU

In December 1999 in Helsinki the European Council decided to develop more effective European military capabilities with a view to undertaking the full range of Petersberg tasks in support of the CFSP. In order to achieve this goal, by the year 2003 the Union was to be able to rapidly deploy units of about 50 000 – 60 000 troops which should be self-sustaining, including the necessary command, strategic reconnaissance and intelligence capabilities. The first steps towards such an autonomous intelligence capability have already been taken in the framework of the WEU and the standing Political and Security Committee. Cooperation among intelligence services within the EU seems essential on the grounds that, firstly, a common security policy which did not involve the secret services would not make sense and, secondly, it would have numerous professional, financial and political advantages. It would also accord better with the idea of the EU as a partner on an equal footing with the United States and could bring together all the Member States in a system which complied fully with the ECHR. The European Parliament would of course have to exercise appropriate monitoring. The European Parliament is in the process of implementing the Regulation (EC) No 1049/2001 on public access to European Parliament, Council and Commission documents by revising the provisions of its Rules of Procedure as regards access to sensitive documents.

13.2. Recommendations

Conclusion and amendment of international agreements on the protection of citizens and firms

1. The Secretary-General of the Council of Europe is called upon to submit to the Ministerial Committee a proposal to protect private life, as guaranteed in Article 8 of the ECHR, brought into line with modern communication and interception methods by means of an additional protocol or, together with the provisions governing data protection, as part of a revision of the Convention on Data Protection, with the proviso that this should neither undermine the level of legal protection established by the European Court of Human Rights nor reduce the flexibility which is vital if future developments are to be taken into account.

2. The Member States of the European Union are called upon to establish a European platform consisting of representatives of the national bodies that are responsible for monitoring Member States' performance in complying with fundamental and citizens' rights in order to scrutinise the consistency of national laws on the intelligence services with the ECHR and the EU Charter of Fundamental Rights, to review the legal provisions guaranteeing postal and communications secrecy, and, in addition, to reach agreement on a recommendation to the Member States on a Code of Conduct to be drawn up which guarantees all European citizens, throughout the territory of the Member States, protection of privacy as defined in Article 7 of the Charter of Fundamental Rights of the European Union and which, moreover, guarantees that the activities of intelligence services are carried out in a manner consistent with fundamental rights, in keeping with the conditions set out in Chapter 8 of this report, and in particular Section 8.3.4., as derived from Article 8 of the ECHR.

3. The member countries of the Council of Europe are called upon to adopt an additional protocol which enables the European Communities to accede to the ECHR or to consider

other measures designed to prevent disputes relating to case law arising between the European Court of Human Rights and the Court of Justice of the European Communities.

4. The Member States are called upon, at the next Intergovernmental Conference, to adopt the EU Charter of Fundamental Rights as a legally binding and enforceable act in order to raise the standard of protection for fundamental rights, particularly with regard to the protection of privacy. The EU institutions are called upon to comply with the fundamental rights laid down in the Charter in their respective areas of responsibility and activity.

5. The European Union and the USA are called upon to conclude an agreement on the basis of which each party applies to the other the rules governing the protection of privacy and the confidentiality of business communications which are valid for its own citizens and firms.

6. The Member States are called upon to conclude an agreement with third countries aimed at providing increased protection of privacy for EU citizens, under which all contracting states give a commitment, where one contracting state intercepts communications in another contracting state, to inform the latter of the planned actions.

7. The UN Secretary-General is called upon to instruct the competent committee to put forward proposals designed to bring Article 17 of the International Covenant on Civil and Political Rights, which guarantees the protection of privacy, into line with technical innovations.

8. The USA is called upon to sign the Additional Protocol to the International Covenant on Civil and Political Rights, so that complaints by individuals concerning breaches of the Covenant by the USA can be submitted to the Human Rights Committee set up under the Covenant. The relevant US NGOs, in particular the ACLU (American Civil Liberties Union) and the EPIC (Electronic Privacy Information Center), are called upon to exert pressure on the US Administration to that end.

9. The Council and the Member States are strongly urged to establish as a matter of priority a system for the democratic monitoring and control of the autonomous European intelligence capability and other joint and coordinated intelligence activities at European level. The European Parliament should play an important role in this monitoring and control system.

National legislative measures to protect citizens and firms

10. The Member States are strongly urged to review their own legislation on the operations of the intelligence services to ensure that it is consistent with the fundamental rights laid down in the ECHR and in the case law of the European Court of Human Rights and, if necessary, to adopt appropriate legal provisions. They are called upon to afford all European citizens the same legal guarantees concerning the protection of privacy and the confidentiality of correspondence. Any of their laws which are discriminatory in terms of the surveillance powers granted to the secret services must be repealed.

11. The Member States are called upon to aspire to a common level of protection against intelligence operations and, to that end, to draw up a code of conduct based on the highest level of protection which exists in any Member State, since as a rule it is citizens of other states, and hence also of other Member States, that are affected by the operations of foreign intelligence services. A similar code of conduct should be negotiated with the USA.

12. The Member States are called upon to pool their communications interception resources with a view to enhancing the effectiveness of the CFSP in the areas of intelligence-gathering and the fight against terrorism, nuclear proliferation or international drug trafficking, in accordance with the provisions governing the protection of citizens' privacy and the confidentiality of business communications, and subject to monitoring by the European Parliament, the Council and the Commission.

Specific legal measures to combat industrial espionage

13. The Member States are called upon to consider to what extent industrial espionage and the payment of bribes as a way of securing contracts can be combated by means of European and international legal provisions and, in particular, whether WTO rules could be adopted which take account of the distortions of competition brought about by such practices, for example by rendering contracts obtained in this way null and void. The USA, Canada, Australia and New Zealand are called upon to join this initiative.

14. The Member States are called upon to give a binding undertaking neither to engage in industrial espionage, either directly or behind the front offered by a foreign power active on their territory, nor to allow a foreign power to carry out such espionage from their territory, thereby acting in accordance with the letter and spirit of the EC Treaty.

15. The Member States and the US Administration are called upon to start an open US-EU dialogue on economic intelligence-gathering.

16. The authorities of the United Kingdom are called upon to explain their role in the UK/USA alliance in connection with the existence of a system of the 'ECHELON' type and its use for the purposes of industrial espionage.

17. The Member States are called upon to ensure that their intelligence services are not misused for the purposes of obtaining competitive intelligence, since this would be at odds with the Member States' duty of loyalty and the concept of a common market based on free competition.

Measures concerning the implementation of the law and the monitoring of that implementation

18. The Member States are called upon to guarantee appropriate parliamentary and legal monitoring of their secret services. Those national parliaments which have no monitoring body responsible for scrutinising the activities of the intelligence services are called upon to set up such a body.

19. The monitoring bodies responsible for scrutinising the activities of the secret services are called upon, when exercising their monitoring powers, to attach great importance to the protection of privacy, regardless of whether the individuals concerned are their own nationals, other EU nationals or third-country nationals.

20. The Member States' intelligence services are called upon to accept data from other intelligence services only in cases where such data has been obtained in accordance with the conditions laid down by their own domestic law, as Member States cannot evade the obligations arising from the ECHR by using other intelligence services.

21. Germany and the United Kingdom are called upon to make the authorisation of further communications interception operations by US intelligence services on their territory conditional on their compliance with the ECHR, i.e. to stipulate that they should be consistent with the principle of proportionality, that their legal basis should be accessible and that the implications for individuals should be foreseeable, and to introduce corresponding, effective monitoring measures, since they are responsible for ensuring that intelligence operations authorised or even merely tolerated on their territory respect human rights.

Measures to encourage self-protection by citizens and firms

22. The Commission and Member States are called upon to inform their citizens and firms about the possibility of their international communications being intercepted. This information must be combined with practical assistance in developing and implementing comprehensive protection measures, not least as regards IT security.

23. The Commission, the Council and the Member States are called upon to develop and implement an effective and active policy for security in the information society. As part of that policy, specific attention should be given to increasing the awareness of all users of modern communication systems of the need to protect confidential information. A Europe-wide, coordinated network of agencies capable of providing practical assistance in designing and implementing comprehensive protection strategies must be established.

24. The Commission and Member States are urged to devise appropriate measures to promote, develop and manufacture European encryption technology and software and above all to support projects aimed at developing user-friendly open-source encryption software.

25. The Commission and Member States are called upon to promote software projects whose source text is made public (open-source software), as this is the only way of guaranteeing that no backdoors are built into programmes. The Commission is called upon to lay down a standard for the level of security of e-mail software packages, placing those packages whose source code has not been made public in the 'least reliable' category.

26. The European institutions and the public administrations of the Member States are called upon systematically to encrypt e-mails, so that ultimately encryption becomes the norm.

Measures to improve security in the institutions

27. The Community institutions and the public administrations of the Member States are called upon to provide training for their staff and make their staff familiar with new encryption technologies and techniques by means of the necessary practical training and courses.

28. The Commission is instructed to have a security analysis carried out which will show what needs to be protected, and to have a protection strategy drawn up.

29. The Commission is called upon to update its encryption system in line with the latest developments, given that modernisation is urgently needed, and calls on the budgetary authority (the Council together with Parliament) to provide the necessary funding.

30. The competent committee is requested to draw up an own-initiative report on security and the protection of secrecy in the European institutions.

31. The Commission is called upon to ensure that data is protected in its own IT systems and to step up the protection of secrecy in relation to documents not accessible to the public.

32. The Commission and the Member States are called upon to invest in new technologies in the field of decryption and encryption techniques as part of the Sixth Research Framework Programme.

Other measures

33. Firms are called upon to cooperate more closely with counter-espionage services, and particularly to inform them of attacks from outside for the purposes of industrial espionage, in order to improve the services' efficiency.

34. The Commission is called upon to put forward a proposal to establish, in close cooperation with industry and the Member States, a Europe-wide, coordinated network of advisory centres - in particular in those Member States where such centres do not yet exist - to deal with issues relating to the security of the information held by firms, with the twin task of increasing awareness of the problem and providing practical assistance.

35. The Commission is called upon to pay particular attention to the position of the applicant countries; if their lack of technological independence prevents them from implementing the requisite protective measures they should be given support.

36. The European Parliament is called upon to hold an international congress on the protection of privacy against telecommunications surveillance in order to provide NGOs from Europe, the USA and other countries with a forum for discussion of the cross-border and international aspects of the problem and coordination of areas of activity and action.