

Withdrawal/Redaction Sheet

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. email	Re: Visit [National Security Act] (2 pages)	09/23/1999	P3/b(3)

COLLECTION:

Clinton Presidential Records
Automated Records Management System [Email]
NSC ([Five Eyes, UKUSA])
OA/Box Number: 1200000

FOLDER TITLE:

[05/21/1999-09/13/2000]

2018-0012-F

in210

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: Jim Kohlenberger (CN=Jim Kohlenberger/O=OVP [UNKNOWN])

CREATION DATE/TIME:21-MAY-1999 11:45:54.00

SUBJECT: Report: U.S. Uses Key Escrow To Steal Secrets

TO: Charlotte Knepper (CN=Charlotte Knepper/OU=NSC/O=EOP@EOP [NSC])

READ:UNKNOWN

TEXT:

As pormised

----- Forwarded by Jim Kohlenberger/OVP on 05/21/99 11:45 AM -----

lc@starium.com

05/19/99 07:09:00 PM

Record Type: Record

To: Jim Kohlenberger@OVP@EOP

cc:

Subject: Report: U.S. Uses Key Escrow To Steal Secrets

Hi Jim,

Just a note to pass along the results of a European Parliament report last Friday.

It seems there is some cynicism regarding the US rationale for restricting encryption software!

All best,

Lee

http://www.nytimes.com/techweb/TW_Report_U_S_Uses_Key_Escrow_To_Steal_Secrets.html

--

Lee Caplin

President & CEO

Starium, Ltd.

225 Cannery Row

Monterey, CA 93940 USA

Tel: +1 831/333.9393 x11

Fax: +1 831/333.9394

===== ATTACHMENT 1 =====

ATT CREATION TIME/DATE: 0 00:00:00.00

TEXT:

<html>

<head>

<title>Report: U.S. Uses Key Escrow To Steal Secrets</title>

```
<meta http-equiv="Expires" content="now">
<meta name="timestamp" content="19990518092700">
<meta name="headline" content="Report: U.S. Uses Key Escrow To Steal Secrets">

<meta name="lead" content="The U.S. has tried to get Europe to adopt encryption
control for U.S. economic gain, says a European Parliament report.">
</head>
<BODY bgcolor="#ffffff" vlink=#444464 link=#000066>

<NYT_HEADER version="1.0" type="main">
<body bgcolor="#ffffff" vlink=#444464 link=#000066 background=http://graphics.n
ytimes.com/images/back.c.gif>

<table border=0 cellpadding=0 cellspacing=0>
<tr><td align=left width=600 valign=top>


<table border=0 cellpadding=0 cellspacing=0>
<td align=left valign=top width=60><br></td>
<td align=left valign=top width=480>
<NYT_BANNER version="1.0" type="main">


</NYT_BANNER>
<br clear=all>
<NYT_TOOLBARMAP version="1.0" type="main">
<map name="maintoolbar2">
<area shape="rect" coords="0,0,75,16" href="/yr/mo/day/"
onMouseOver="window.status='Click to go to the Home Page';return true">
<area shape="rect" coords="76,0,154,16" href="/info/contents/siteindex.html"
onMouseOver="window.status='Click to see site contents';return true">
<area shape="rect" coords="155,0,233,16" href="/search/daily/"
onMouseOver="window.status='Click to search the current site';return true">
<area shape="rect" coords="234,0,312,16" href="/comment/"
onMouseOver="window.status='Click for discussion in the Forums';return true">
<area shape="rect" coords="313,0,391,16" href="/archives/"
onMouseOver="window.status='Click to search the archives';return true">
<area shape="rect" coords="392,0,468,16" href="/marketplace/"
onMouseOver="window.status='Click to visit the Marketplace';return true">
</map>

</NYT_TOOLBARMAP>
<NYT_TOOLBAR version="1.0" type="main">
<a href="/images/maintoolbar2.map">
</a>

</NYT_TOOLBAR>
<br><NYT_AD version="1.0" location="top">

<A HREF="http://images2.nytimes.com/RealMedia/ads/click_lx.ads/www.nytimes.com/
techweb/TW_Report_U_S_Uses_Key_Escrow_To_Steal_Secrets.html/0/Top/micnit04/ntr1
0-head.gif/63653337653133613337343334663730" target="_top"><IMG SRC="http://ima
ges2.nytimes.com/RealMedia/ads/adstream_lx.ads/www.nytimes.com/techweb/TW_Repor
t_U_S_Uses_Key_Escrow_To_Steal_Secrets.html/0/Top/micnit04/ntr10-head.gif/63653
337653133613337343334663730" border=0 WIDTH=468 HEIGHT=60 ALT="Microsoft.com"
></A>
```

```
</NYT_AD>
</td></table>
```

```
</NYT_HEADER>
<BLOCKQUOTE><BLOCKQUOTE>
```

```
<NYT_DATE version="1.0">
<h5>May 18, 1999</h5><br>
</NYT_DATE>
```

```
<NYT_HEADLINE version="1.0" type="main">
<h2>Report: U.S. Uses Key Escrow To Steal Secrets</h2>
</NYT_HEADLINE>
```

```
<p><b>Filed at 9:27 a.m. EDT</b><p>
<NYT_BYLINE version="1.0">
<h5>By Madeleine Acey for <a href=http://www.techweb.com>TechWeb</a>, CMPnet</h5>
</NYT_BYLINE>
```

```
<NYT_TEXT version="1.0">
```

```
<form method="POST" action="http://www.techweb.com/search/multiSearch">
<table border=0 align=right cellspacing=6 cellpadding=8 bgcolor=#cccccc>
<tr><td align=left valign=top>
<b><font size=-1 color=ab0000><B>RESOURCES</B></font></b><br>
<FONT SIZE="1">From CMPnet</FONT>
<hr size=1>
<input name="type" value="Encyclopedia" type="radio"> <FONT SIZE="-1">Encyclope
dia</FONT><br>
<input name="type" value="Products" type="radio"> <FONT SIZE="-1">Product Revie
ws</FONT><br>
<input name="type" value="Downloads" type="radio"> <FONT SIZE="-1">Downloads</F
ONT><br>
<INPUT TYPE="text" NAME="search_term" SIZE="12">
<br>
<INPUT TYPE="submit" VALUE="Search">
</tr></td>
</table>
</FORM>
```

```
<P>
European plans for controlling encryption software are nothing to do with law e
nforcement and everything to do with U.S. industrial espionage, according to a
report released by the European Parliament on Friday.<P></P>
<P>The working document for the Scientific and Technological Options Assessment
panel said the United States has tried to persuade European Union countries to
adopt its key escrow or key recovery policies -- allowing backdoor access to e
ncryption programs -- saying this was necessary to read messages exchanged by c
riminals.<P></P>
<P>But the report details how the UKUSA alliance -- made up of the United Kingd
om, United States, Canada, Australia, and New Zealand -- has used its secret Ec
helon global spying network to intercept confidential company communications an
d give them to favored competitors. Thomson S.A., located in Paris, and Airbus
Industrie, based in Blagnac Cedex, France, are said to have lost contracts as a
result of information passed to rivals.<P></P>
<P>"The U.S. government misled states in the EU and [Organization for Economic
Cooperation and Development] about the true intention of its policy," the repor
t adds.<P></P>
```

<P>"Between 1993 and 1997 police representatives were not involved in the NSA [National Security Agency]-led policy-making process for key recovery. Despite this, during the same period the U.S. government repeatedly presented its policy as being motivated by the stated needs of law-enforcement agencies."<P></P>

<P>The document went on to detail how the agencies specifically studied Internet data. Apart from scanning all international communications lines -- using 120 satellites, microwave listening stations, and an adapted submarine -- it said they stored and analyzed Usenet discussions. "In the U.K., the Defence Evaluation and Research Agency maintains a 1-terabyte database containing the previous 90 days of Usenet messages."<P></P>

<P>The "NSA employs computer 'bots' (robots) to collect data of interest," the report adds. "For example, a New York website known as JYA.COM offers extensive information on cryptography and government communications interception activities. Records of access to the site show that every morning it is visited by a bot from NSA's National Computer Security Center, which looks for new files and makes copies of any that it finds."<P></P>

<P>According to a former employee, NSA had by 1995 installed "sniffer" software to collect traffic at nine major Internet exchange points.<P></P>

<P>The report offered evidence that a leading U.S. Internet and telecommunications company had contracted with the NSA to develop software to capture Internet data of interest, and that deals had been struck with Microsoft, Lotus, and Netscape to alter their products for foreign use.<P></P>

<P>"There can't be any doubt any longer that there's an economic imperative to these policies," said Simon Davies, director of Privacy International. "We have been lied to for years. But it will be up to companies like Airbus to take legal action to force a definition of national security in the context of the European Union. Then we can establish a legal framework and appeals process."<P></P>

<P>Meanwhile, the Financial Times reported on Monday that the U.K. government had agreed to take key escrow "off the agenda" and had accepted industry proposals for a "largely voluntary program of co-operation with the security services".<P></P>

<P>Government officials could not confirm the report.<P></P>

<P>But Caspar Bowden, director of the Foundation for Information Policy Research, questioned how far any compromise would go. "Will they persist with statutory licensing [of trusted third parties] and criminal legislation on decryption warrants?" he asked.<P></P>

<P>Andrew Dornan of Data Communications International contributed to this report. </P>

<P>(c) 1999 CMP Media Inc.

</P>

</NYT_TEXT>

<NYT_FOOTER version="1.0">

</BLOCKQUOTE></BLOCKQUOTE>

<table border=0 cellpadding=0 cellspacing=0>

<td align=left valign=top width=60>
</td>

<td align=center valign=top width=468>

<NYT_AD version="1.0" location="bottom">

<IMG SRC="http://images2.nytimes.com/RealMedia/ads/adstream_lx.ads/www.nytimes.com/techweb/TW_Report_U_S_Uses_Key_Escrow_To_Steal_Secrets.html/0/Bottom/micnit04/ntr10-3tal.gif

/63653337653133613337343334663730" border=0 WIDTH=468 HEIGHT=60 ALT="Microsoft.com" >

</NYT_AD>

<hr size=1>

<P>

<NYT_TOOLBAR version="1.0" type="main">

Home |

Site Index |

Site Search |

Forums |

Archives |

Marketplace

<P>

Quick News |

Page One Plus |

International |

National/N.Y. |

Business |

Technology |

Science |

Sports |

Weather |

Editorial |

Op-Ed |

Arts |

Automobiles |

Books |

Diversions |

Job Market |

Real Estate |

Travel

<P>

Help/Feedback |

Classifieds |

Services |

New York Today

</NYT_TOOLBAR>

<NYT_COPYRIGHT version="1.0" type="main">

<P>

Copyright 1999 The New York Times Company

<P> The information contained in this CMPnet news report
may not be republished or redistributed
without the prior written authority of CMPnet.

</NYT_COPYRIGHT>

</td></table>

</td>

<td align=left width=14 valign=top>

</td>

<td align=center width=140 valign=top>

<table width="140" border="0" cellpadding="0" cellspacing="0">

```
<tr><td width="140"><a href="http://images2.nytimes.com/RealMedia/ads/click_lx.
ads/www.nytimes.com/techweb/TW_Report_U_S_Uses_Key_Escrow_To_Steal_Secrets.html
/0/Right3/winetoday_side/wt11.html/63653337653133613337343334663730?_RM_REDIRE
winetoday.com"></a><br clear=all>
```

```
<!-- begin inner table -->
```

```
<table width="140" border="0" cellspacing="0" cellpadding="0">
<tr>
<td width="1" rowspan="10" bgcolor="#000000"></td>
<td width="4" rowspan="10" bgcolor="#ffffff"></td>
<td width="130" bgcolor="#ffffff"><br clear=all>
<a href="http://images2.nytimes.com/RealMedia/ads/click_lx.ads/www.nytimes.com/
techweb/TW_Report_U_S_Uses_Key_Escrow_To_Steal_Secrets.html/0/Right3/winetoday_
side/wt11.html/63653337653133613337343334663730?_RM_REDIRE=winetoday.com/review
sindex.html"></a></td>
```

```
<td width="4" rowspan="10" bgcolor="#ffffff"></td>
<td width="1" rowspan="10" bgcolor="#000000"></td>
```

```
</tr>
```

```
<tr>
```

```
<td width="130" bgcolor="#ffffff"><font size="2" color="#336699">
<center><b><i>Search Our Reviews</i></b></center>
<font co
lor="#00066">Merlots</font></a><br clear=all>
 • <a href="http://winetoday.com/reviews/searchresults
2.asp?varietal=Cabernet&editorialChoices=Cellar+Worthy+Wine&priceRange=5"><font
color="#00066">Cabernets</font></a> Fit for<br clear=all>
 the Cellar<br clear=all>
 • Four-Star <a href="http://images2.nytimes.com/RealM
edia/ads/click_lx.ads/www.nytimes.com/techweb/TW_Report_U_S_Uses_Key_Escrow_To_
Steal_Secrets.html/0/Right3/winetoday_side/wt11.html/63653337653133613337343334
663730?_RM_REDIRE=winetoday.com/reviews/searchresults2.asp?varietal=Viognier&ra
ting=4"><font color="#00066">Viogniers</font></a><br clear=all>
 • Russian River<br clear=all>
 • <a href="http://winetoday.com/reviews/searchresults2.asp
?varietal=Pinot+Noir&appellation=Russian+River+Valley"><font color="#00066">Pino
t Noirs</font></a><br clear=all>
 • Buttery <br clear=all>
 <a href="http://winetoday.com/reviews/searchresults2.asp?
varietal=Chardonnay&qualities3=butter"><font color="#00066">Chardonnays</font><
/a><br clear=all>
<br clear=all>
```

```
 • Custom <a href="http://winetoday.com/reviews/advanc
edsearch.asp"><font color="#00066">Search</font></a><br clear=all>
 • Wine of the <a href="http://winetoday.com/wineofthe
week/"><font color="#00066">Week</a></font><br clear=all>
 • Wine Reviews for<br clear=all>
 Your <a href="http://winetoday.com/palm/"><font color="#
00066">PalmPilot</font></a><br clear=all>
```

```
<center><a href="http://winetoday.com/reviews/searchresults2.asp?editorialchoic
es=cellar+worthy+wine"></a></center
>
</font>
</td>
</tr>
```

```
<tr>
<td width="130" bgcolor="#ffffff"><br clear=all>
<a href="http://winetoday.com/sectionfronts/events.asp"></a>
</td>
</tr>
```

```
<tr>
<td width="130" bgcolor="#ffffff"><font size="2" color="#336699">
 • <a href="http://winetoday.com/sectionfronts/events2
.asp?keyword=New+York"><font color="#00066">New York</font></a> Events<br clear
=all>
 • Search <a href="http://winetoday.com/sectionfronts/
events.asp"><font color="#00066">All</font></a> Events<br clear=all>
 • <a href="http://winetoday.com/events/addNewEvent.as
p"><font color="#00066">Add</font></a> Your Event<br clear=all>
</td>
</tr>
```

```
<tr>
<td width="130" bgcolor="#ffffff"><br clear=all>
<a href="http://winetoday.com/newsmain.html"></a>
</td>
</tr>
```

```
<tr>
<td width="130" bgcolor="#ffffff"><font size="2" color="#336699">
 • Feature <a href="http://winetoday.com/sectionfronts
/opinion.asp"><font color="#00066">Stories</font></a><br clear=all>
 • Special <a href="http://winetoday.com/sectionfronts
```

```
/specialreports.asp"><font color="#00066">Reports</font></a><br clear=all>
 • <a href="http://winetoday.com/sectionfronts/auction
sevents.asp"><font color="#00066">Auction</font></a> & Events<br clear=all>
</td>
</tr>

<tr>
<td width="130" bgcolor="#ffffff"><br clear=all>
<a href="http://winetoday.com/wineriesindex.html"></a>
</td>
</tr>

<tr>
<td width="130" bgcolor="#ffffff"><font size="2" color="#336699">
 • <a href="http://winetoday.com/winery/searchresults2
.asp?editorialChoices=Cellar+Worthy+Producer"><font color="#00066">Cellar</font
></a> Worthy<br clear=all>
 • Upcoming <a href="http://winetoday.com/winery/searc
hresults2.asp?editorialChoices=Upcoming+Star"><font color="#00066">Stars</font>
</a><br clear=all>
 • <a href="http://winetoday.com/winery/searchresults2
.asp?editorialChoices=Good+Value+Producer"><font color="#00066">Value</font></a
> Producer<br clear=all>
 • Custom <a href="http://winetoday.com/winery/advance
dsearch.asp"><font color="#00066">Search</font></a></font>
</td>
</tr>

<tr>
<td width="130" align="CENTER" bgcolor="#FFFFFF"><br cl
ear=all>
<a href="http://winetoday.com/contests.html"></a></td>
</tr>

<tr>
<td width="130" bgcolor="#ffffff"><font size="2" color="#336699">
 • Win an Instant <br clear=all>
 <a href="http://winetoday.com/contests.html"><font color
="#00066">Wine Cellar</font></a>!<br clear=all>
 • Win Event <a href="http://winetoday.com/contests.h
tml"><font color="#00066">Tickets</font></a><br clear=all>

<br>

<center>
```

```
</center>
</td>
</tr>
```

```
<tr>
<td colspan="5" width="140" bgcolor="#000000"></td>
</tr>
```

```
</table>
```

```
<!-- end inner table -->
```

```
</table>
</td>
</tr>
</table>
```

```
</td></tr></table>
```

```
</NYT_FOOTER>
```

```
</BODY>
</HTML>
```

```
===== END ATTACHMENT 1 =====
```

```
===== ATTACHMENT 2 =====
ATT CREATION TIME/DATE: 0 00:00:00.00
```

TEXT:

RFC-822-headers:

Received: from conversion.pmdf.eop.gov by PMDF.EOP.GOV (PMDF V5.1-9 #D3421)
id <01JBE78FLMFK0006LA@PMDF.EOP.GOV> for Kohlen_j@a1.eop.gov; Wed,
19 May 1999 20:16:57 EST

Received: from storm.eop.gov by PMDF.EOP.GOV (PMDF V5.1-9 #D3421)
with ESMTP id <01JBE78C0R5C0007HK@PMDF.EOP.GOV> for Kohlen_j@a1.eop.gov; Wed,

19 May 1999 20:16:52 -0500 (EST)

Received: from relay.starium.com ([206.55.225.50])
by EOP.GOV (PMDF V5.2-31 #34437) with ESMTP id <01JBE77FWDG6000RJX@EOP.GOV>
for Kohlen_j@a1.eop.gov; Wed, 19 May 1999 20:16:14 -0500 (EST)

Received: from starium.com (krypton.starium.com [206.55.225.58])
by relay.starium.com (8.8.7/8.8.7) with ESMTP id QAA29259 for
<Kohlen_j@a1.eop.gov>; Wed, 19 May 1999 16:52:42 -0700

X-Mailer: Mozilla 4.05 [en] (Win95; I)

```
===== END ATTACHMENT 2 =====
```

Withdrawal/Redaction Marker

Clinton Library

DOCUMENT NO. AND TYPE	SUBJECT/TITLE	DATE	RESTRICTION
001. email	Re: Visit [National Security Act] (2 pages)	09/23/1999	P3/b(3)

COLLECTION:

Clinton Presidential Records
Automated Records Management System [Email]
NSC ([Five Eyes, UKUSA])
OA/Box Number: 1200000

FOLDER TITLE:

[05/21/1999-09/13/2000]

2018-0012-F

jn210

RESTRICTION CODES

Presidential Records Act - [44 U.S.C. 2204(a)]

- P1 National Security Classified Information [(a)(1) of the PRA]
- P2 Relating to the appointment to Federal office [(a)(2) of the PRA]
- P3 Release would violate a Federal statute [(a)(3) of the PRA]
- P4 Release would disclose trade secrets or confidential commercial or financial information [(a)(4) of the PRA]
- P5 Release would disclose confidential advice between the President and his advisors, or between such advisors [(a)(5) of the PRA]
- P6 Release would constitute a clearly unwarranted invasion of personal privacy [(a)(6) of the PRA]

C. Closed in accordance with restrictions contained in donor's deed of gift.

PRM. Personal record misfile defined in accordance with 44 U.S.C. 2201(3).

RR. Document will be reviewed upon request.

Freedom of Information Act - [5 U.S.C. 552(b)]

- b(1) National security classified information [(b)(1) of the FOIA]
- b(2) Release would disclose internal personnel rules and practices of an agency [(b)(2) of the FOIA]
- b(3) Release would violate a Federal statute [(b)(3) of the FOIA]
- b(4) Release would disclose trade secrets or confidential or financial information [(b)(4) of the FOIA]
- b(6) Release would constitute a clearly unwarranted invasion of personal privacy [(b)(6) of the FOIA]
- b(7) Release would disclose information compiled for law enforcement purposes [(b)(7) of the FOIA]
- b(8) Release would disclose information concerning the regulation of financial institutions [(b)(8) of the FOIA]
- b(9) Release would disclose geological or geophysical information concerning wells [(b)(9) of the FOIA]

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: "Kurtz, James" <JKurtz@ida.org> ("Kurtz, James" <JKurtz@ida.org> [UNKNOWN

CREATION DATE/TIME:15-DEC-1999 10:53:58.00

SUBJECT: For What It's Worth

TO: Mark C. Montgomery (CN=Mark C. Montgomery/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TEXT:

Date: 12/14/99 11:17 PM

From: MTClubb02

Surveillance Society: Exposing Echelon

By Erin Zimmerman

December 14, 1999

-- A Russian spy made headlines last week after he was found listening in on conversations through a bug planted at the U.S. State Department, and there are renewed concerns about Chinese spying.

But the government is using methods that are far more sophisticated -- and far more secret -- to capture everything from phone calls to e-mails to faxes. And there's growing evidence that they may be using it, not just on terrorists, but on you.

"I think that people need to understand that we're entering an age of a new America, and we're not going to like it," says privacy expert Lisa Dean of the Free Congress Foundation. "This is not a society where what we say, or what we do, or what we tell people is kept a secret."

"And people's conversations are being eavesdropped on in violation of the 4th amendment," says Greg Nojeim of the American Civil Liberties Union. "If Americans don't wake up to their diminishing window of privacy, as it were, pretty soon, there's not going to be any left."

In a high-tech world that now contains 40 million cell phones, 14 million fax machines, and 180 million computers, just how private is your communication? The answer may surprise you.

"I don't think we have a whole lot of privacy left in America," says Dean. "We think we do, but we really don't."

Big Brother may not be watching yet ... but he may be listening to your phone calls and reading your e-mail, all in the name of national security.

"Secretary of Defense William Cohen has said publicly, the American people need to decide how much privacy they're willing to give up in favor of more security," says Dean. "Well, the answer to that should be none."

And as Americans move further into the information age, Big Brother is rapidly becoming public enemy number one.

"The Wall Street Journal conducted a poll about a month ago and asked Americans what do you fear most in the next century. Terrorism? No. Crime? No. The thing that concerned most Americans was the loss of personal privacy."

At the center of the firestorm over electronic privacy is the National Security Agency, headquartered in Fort Meade, Maryland. With a global staff of around 38,000 the NSA is larger than the FBI and the CIA combined.

"The NSA has two missions: one is foreign intelligence gathering, and the other one is creation of codes to protect U.S. diplomatic and military secrets," says former NSA analyst Wayne Madsen. "Historically, that's been NSA's two major functions. Unfortunately, with the end of the Cold War, they're now looking into other areas."

These other areas may include your own home, through a global eavesdropping system known as ECHELON.

"What ECHELON basically is is a system that, based on key words in a conversation or key words in an e-mail -- it takes those key words of interest, which are basically pre-programmed in something called a dictionary."

According to Madsen, this dictionary may be searching your phone calls, faxes, and e-mails to sniff out terrorists, hackers, and other potential threats. Privacy experts charge that even accidental use of these so-called key words could put you under the sharp ears of the NSA.

"I think the NSA would say, 'I wonder what they're up to,' and I think there might be increased monitoring of their communications."

Most of the public information about ECHELON is based on a report commissioned by the European parliament.

Published last April, the report charges that the NSA's global spy bases, like the one at Menwith Hill in England, routinely intercept around two-million communications every hour.

"So basically, you can think of it as a giant drift net that captures everything," says Madsen.

The countries casting this global drift net are members of what's known as the UKUSA alliance: the United States, Canada, Australia, New Zealand, and the United Kingdom. According to the EU report, this five-pronged partnership also forms the legal loophole that allows the NSA to spy on its own citizens. "The NSA has no jurisdiction here in this country," says Dean.

"So it can't legally listen in on Americans' phone conversations or electronic communications. However, according to the European parliament, what it's doing is getting its British counterparts, or Australian counterparts, and so on, to do their dirty work." For example, if you send an e-mail message from New York to Los Angeles, it may be routed through Canada or the UK before reaching its destination. And once a message travels outside U.S. borders, it's fair game for ECHELON's web.

Most Americans got their first glimpse of the super-secret agency in the 1998 action film *Enemy of the State*. Former attorney and journalist James Bamford wrote *The Puzzle Palace*, considered to be the definitive work on the NSA. And although film producers relied heavily on his best-selling book to make *Enemy of the State*, Bamford says they used more than a little creative license.

"The NSA doesn't possibly have the ability to do that," says Bamford.

"There

are too many inaccuracies. NSA doesn't control imagery satellites, photo satellites -- you don't pick up the phone and say, 'I want a satellite on the corner of Wisconsin and M Street, and they don't go into hotel rooms -- they can't do hotel rooms, so there were a lot of problems I had with it."

Meanwhile, critics are asking, if the Cold War is over, then why has global intelligence continued to mushroom?

"Russia's defeated; we are still the superpower, the one and only superpower

in the world," says Dean. "How do we justify all the systems that we have in

place; how do we justify all of the activities of the people we've employed in the intelligence community to keep going?"

But Bamford, an NSA observer for over 20 years, argues that there are still too many global hotspots to consider downsizing at Fort Meade. For example, while much of the NSA's attention was focused on the growing missile threats

in North Korea, it completely missed the budding nuclear rivalry between India and Pakistan in 1998.

"This is an intelligence agency that some critics are giving enormous abilities to listen to everything everywhere at all times; but this was a major security issue, whether India and Pakistan were developing nuclear weapons, but they didn't hear it -- they didn't know about it," he says.

"So

this is an agency that is given far more credit for being able to listen to things than they are able to. They can't even listen to things they're supposed to be listening to, let alone things they're not supposed to be listening to."

Since its creation in 1952, the National Security Agency has remained America's biggest intelligence secret -- so secret, in fact, that Washington

insiders often joke that the initials "NSA" stand for "No Such Agency." But for the first time in its history, the agency may be forced to reveal some of those secrets to Congress.

Georgia Republican Bob Barr is leading a congressional movement to force the

NSA to answer for spying on U.S. citizens.

"There seems to be very credible evidence that this operation is taking place, and has been taking place for quite some time," says Barr. "At this point, all we're asking for is the basic information telling us what do you at the NSA, the National Security Agency, believe is the legal basis for you

to gather this information? That's the starting point: What's the basis that

you believe you're authorized to do this?"

That question set off a battle royal between the NSA and the House Intelligence Committee earlier this year. When asked about the legality of their procedures, the agency refused to provide Congress with any information, citing attorney-client privilege.

"It's hard to say it with a straight face," says Barr. "They just make these

things up in order to not disclose something they don't want to disclose."

"Even people on the inside at NSA realize that that was a terrible mistake they made by trying to invoke client-attorney privilege to try to avoid providing Congress answers to questions that Congress asked them," says Madsen.

In response, Barr proposed a measure that will require the NSA to report to Congress on the legal standards they use for spying. The measure was passed by the House and is now under consideration by the Senate. Congressional hearings on ECHELON are expected early next year.

Meanwhile the battle against Big Brother has forged some unusual alliances in Washington. At Barr's side in this investigation is the American Civil Liberties Union, which is working hard to make ECHELON a household name on Capitol Hill. In November, the ACLU went online with a watchdog Web site designed to put the American public on "ECHELON Watch." The Web site can be found at www.echelonwatch.org.

"The NSA is used to operating in a black box," says Nojeim. "When it comes to our rights, that box needs to be opened. The only people who can open that box for the American people are the members of Congress."

NSA officials declined an interview with CBN News, but sent a written statement saying, "The National Security Agency operates in strict accordance with U.S. laws in protecting the privacy rights of U.S. persons."

Congress is now faced with the challenge of finding hard evidence about how the program operates, a difficult task since the agency's official position is that it can neither "confirm or deny the existence of ECHELON."

And despite numerous outside allegations about the NSA's spying activities, no one on the inside has been willing to talk publicly about ECHELON ... until now.

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: JIM LEWIS <JLEWIS@bxa.doc.gov> (JIM LEWIS <JLEWIS@bxa.doc.gov> [UNKNOWN]

CREATION DATE/TIME:15-FEB-2000 13:29:40.00

SUBJECT: Re: SLIDES

TO: Charlotte Knepper (CN=Charlotte Knepper/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TEXT:

While you're waiting - from the London Times...

French to sue US and Britain over network of spies

FROM ADAM SAGE IN PARIS

THE British and US Governments are to be sued in France after claims that they have spied on French companies, diplomats and Cabinet ministers. Lawyers are planning a class action after confirmation last week that a global anglophone spy network exists.

Codenamed P-415 Echelon, the world's most powerful electronic spy system was revealed in declassified US National Security Agency documents published on the Internet, and is capable of intercepting telephone conversations, faxes and e-mails.

The system was established in the 1980s by the UKUSA alliance, which unites the British, American, Australian, New Zealand and Canadian secret services. In Europe, its listening devices are at Menwith Hill defence base in Yorkshire. French MPs claim to have evidence that the European Airbus consortium lost a Fr35 billion (æ3.5 billion) contract in 1995 after its offer was overheard and passed to Boeing. Georges Sarre, a left-wing MP, said: "The participation of the United Kingdom in spying on its European partners for and with the US raises serious and legitimate concerns in that it creates a particularly acute conflict of interest within the European Union."

The European Parliament's Civil Liberties Committee will study a report on the Echelon network on February 23. The debate is certain to fuel criticism of Britain's role.

Until this month, the network was an official secret recognised by none of the members of the UKUSA alliance. But the documents published by the George Washington University prove its existence and its capacity to intercept civilian satellite communications.

Jean-Pierre Millet, a Parisian lawyer, said that Echelon tracked every mobile and satellite call, but only decoded those involving a key figure. "You can bet that every time a French government minister makes a mobile phone call, it is recorded," he said.

M Millet said that Echelon's system leaves it open to legal challenge under French privacy laws. "The simple fact that an attempt has been made to intercept a communication is against the law in France, however the information is exploited." Yesterday he said that he would bring an action on behalf of French civil liberty groups.

>>> <Charlotte_Knepper@nsc.eop.gov> 02/15/00 10:29AM >>>
Please send slides monsieur.

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: allan berg <bergax@cs.jmu.edu> (allan berg <bergax@cs.jmu.edu> [UNKNOWN]

CREATION DATE/TIME:20-FEB-2000 17:33:01.00

SUBJECT: (ai) Canada: new space invaders Spies in the sky (fwd)

TO: Mark C. Montgomery (CN=Mark C. Montgomery/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TO: Jeffrey A. Hunker (CN=Jeffrey A. Hunker/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TEXT:

Allan Berg

Director, INFOSEC Program Office

bergax@jmu.edu

O) 540.568.8773

F) 540.568.6023

WWW.INFOSEC.JMU.EDU

----- Forwarded message -----

Date: Sun, 20 Feb 2000 12:31:39 EST

From: WILSONGI@aol.com

To: ACCESS@g2-forward.org, nipmail@xmission.com

Subject: (ai) Canada: new space invaders Spies in the sky

The new space invaders Spies in the sky

Peter Goodspeed

National Post

<http://www.nationalpost.com/news.asp?s2=worlds3=observer&f=000219/210021.html>

A former employee of Canada's security agency has charged that Canadian spies

once managed to overhear the American ambassador to Canada discussing a pending trade deal with China on a mobile telephone and used that information

to undercut the Americans in landing a \$2.5-billion Chinese grain sale.

For decades they were guardians -- mysterious warriors who straddled the globe searching for secrets that would prevent a nuclear holocaust. But now, the new technology of the post-Cold War world has suddenly transformed the West's leading spymasters into sinister shadows manipulating a massive surveillance system that can capture and study every telephone call, fax and e-mail message sent anywhere in the world.

These high-tech espionage agents from Canada, the United States, Britain, Australia and New Zealand -- backed up by a web of ships, planes and radar and communication interception sites, that ring the earth -- have established the greatest spy network in history. Its name is Echelon.

Originally devoted solely to monitoring the military and diplomatic communications of the Soviet Union and its East Bloc allies, today Echelon searches for hints of terrorist plots, drug-dealer's plans and political

and diplomatic intelligence. But critics claim the system is also being used for crass commercial theft and a brutal invasion of privacy on a staggering scale.

On Tuesday, the European Union's parliament will open a major international debate on the spy practices of the world's five leading English-speaking nations, claiming that this electronic espionage ring, led by the United States and Britain, is methodically going where it has no right to go. The EU's civil liberties committee is expected to accuse Britain of aiding the United States in conducting economic and commercial espionage on a grand scale at the expense of its European partners. A special 112-page expose of the spy network prepared for the EU last spring declares that the rapid proliferation of surveillance technologies presents "a serious threat to the civil liberties in Europe" with "awesome implications."

"There is wide-ranging evidence indicating that major governments are routinely utilizing communications intelligence to provide commercial advantage to companies and trade," declared Duncan Campbell, the report's author, a Scottish physicist and researcher who has devoted 20 years to studying electronic espionage.

Moreover, research about to be released by the EU's Scientific and Technical Options Assessment office is expected to document how deeply Echelon has penetrated Europe. It will outline ways to combat the espionage assault.

At the same time:

- Jean-Pierre Millet, a Parisian lawyer, has launched a class-action lawsuit against the governments of the United States and Britain, claiming the Echelon spy network has robbed European industries of some of their most cherished trade secrets and undercut their bargaining positions in trade deals.
- Parliamentarians in Italy, Germany and Denmark are demanding public investigations of the spy network.
- Privacy advocates in the U.S. have launched a court case demanding access to government documents on Echelon under the Freedom of Information Act.
- Several leading politicians are calling for the first Congressional hearings to review U.S. intelligence-gathering practices since the Watergate era.
- On the Internet, privacy advocates, computer hackers and journalists are engaged in near-hysterical searches for signs of Echelon's presence. Several new Internet Web sites have sprung up devoted solely to documenting information on Echelon and pressing for public investigations into the surveillance system.

"Echelon is a black box, and we really don't know what is inside it," says Barry Steinhardt, of the American Civil Liberties Union. "We don't know who is being targeted, what they are being targeted for or what is being done with the information."

The Echelon system is simple in design. All members of the English-speaking alliance are part of the UKUSA intelligence alliance that has maintained ties since the Second World War. These states have positioned electronic-intercept stations and deep-space satellites to capture all satellite, microwave, cellular and fibre-optic communications traffic. The captured signals are then processed through a series of supercomputers, known as dictionaries, that are programmed to search each communication for targeted addresses, words, phrases or even individual voices.

Individual states in the UKUSA alliance are assigned responsibilities for monitoring different parts of the globe. Canada's main task used to be monitoring northern portions of the former Soviet Union and conducting sweeps of all communications traffic that could be picked up from our embassies around the world. In the post-Cold War era, a greater emphasis has been placed on monitoring satellite and radio and cellphone traffic originating from Central and South America, primarily in an effort to track drugs and thugs in the region.

The United States, with its vast array of spy satellites and listening posts, monitors most of Latin America, Asia, Asiatic Russia and northern China. Britain listens in on Europe and Russia west of the Urals as well as Africa. Australia hunts for communications originating in Indochina, Indonesia and southern China. New Zealand sweeps the western Pacific.

"Most people just don't understand how pervasive government surveillance is," warns John Pike, a leading military analyst with the Washington-based American Federation of Scientists. "If you place an international phone call, the odds that the [U.S.] National Security Agency are looking is very good. If it goes by oceanic fibre-optic cable, they are listening to it. If it goes by satellite, they are listening to it. If it is a radio broadcast or a cellphone conversation, in principle, they could listen to it. Frankly, they can get what they want."

Experts stress that Echelon is simply a method of sorting captured signals and is just one of the many new arrows in the intelligence community's quiver, along with increasingly sophisticated bugging and interception techniques, satellite tracking, through-clothing scanning, automatic fingerprinting and recognition systems that can recognize genes, odours or retina patterns.

The Americans dominate the UKUSA alliance, providing most of the computer expertise and frequently much of the personnel for global interception bases. The U.S. National Security Agency, headquartered in Fort Meade, Md., just outside Washington, has a global staff of 38,000 and a budget estimated at more than \$3.6-billion (all dollar figures US unless otherwise specified). That's more than the FBI and the CIA combined.

By comparison, Canada's communications-intelligence operations are conducted

by the Communications Security Establishment (CSE), a branch of the National Defence Department. It has a staff of 890 people and an annual budget of \$110-million (Cdn). The CSE's headquarters, nicknamed "The Farm," is the Sir Leonard Tilley Building on Heron Road in Ottawa, and its main communications intercept site is located on an old armed-forces radio base in Leirtrim, just south of Ottawa.

Though shrouded in secrecy to the extent that American officials used to joke NSA stood for "No Such Agency" or "Never Say Anything," few foreign-affairs analysts are surprised by the sweep or appetite of electronic spies and they caution against taking Europe's angry protestations of dismay at face value.

"The EU hearings are a bit of a joke," says Wayne Madsen, a former NSA employee and senior fellow at the Washington-based Electronic Privacy Information Centre (EPIC). "It's going to be a bit like that scene in the movie Casablanca, where Inspector Renault declares: 'I'm shocked to find gambling in this establishment.' "

"The fact is the German Greens and the French Socialists and Gaullists can pull their hair out and say, 'This is terrible,' but their countries are involved in this stuff. The French have an extensive signals intelligence network of their own. I think what is going to happen is there will be a lot of wringing of hands and gnashing of teeth, but then business is going to go on as usual."

But the real issue is whether UKUSA's spies are using electronic espionage to get commercial information.

"Since the demise of Communism in Eastern Europe, the intelligence agencies have searched for a new justification for their surveillance capability in order to protect their prominence and their bloated budgets," says Patrick Poole, deputy director of the Centre of Technology at Washington's Free Congress Federation. "Their solution was to redefine the notion of national security to include economic, commercial and corporate concerns.

"By redefining the term 'national security' to include spying on foreign competitors of prominent U.S. corporations, the signals-intelligence game has gotten ugly."

Lately there has been a frenzy of concern over possible American economic espionage in Europe.

- Yesterday, a French intelligence report accused U.S. secret agents of working with computer giant Microsoft to develop software allowing Washington to spy on computer users around the world. It claims that the National Security Agency helped install secret programs on Microsoft software, currently in use of 90% of computers.

- In 1990 the German newsmagazine Der Spiegel claimed NSA intercepted messages about a pending \$200-million telecommunications deal between Indonesia and the Japanese satellite manufacturer NEC Corp. George Bush, then the U.S. president, is said to have intervened on the basis of the intelligence intercept and to have convinced the Indonesians to split the contract between NEC and U.S.-owned AT&T.

- Last spring's EU report on electronic spying says that U.S. intelligence agencies intercepted phone calls between Brazilian officials and the French firm Thomson-CSF in 1994 and used the information to swing a \$1.3-billion radar contract to the U.S. corporation Raytheon.

Mike Frost, a former CSE employee and author of Spyworld, which is about his career in Canada's secret service, claims that as far back as 1981 Canada was using its U.S.-produced spy technology to eavesdrop on the American ambassador to Ottawa. In one instance, Canadian spies managed to overhear the ambassador discussing a pending trade deal with China on a mobile telephone and used that information to undercut the Americans in landing a \$2.5-billion Chinese grain sale.

On another occasion, in 1983, Mr. Frost says British intelligence officials invited their Canadian counterparts to come to London to eavesdrop on two British cabinet ministers whose political loyalty was doubted by Margaret Thatcher, then the British prime minister. Since it would have been illegal for British officials to do the surveillance themselves, they had the Canadians do the job using eavesdropping equipment in the Canadian embassy. After three weeks of snooping, the Canadians quietly turned over all their findings to the British, Mr. Frost says.

"It should hardly be surprising that Echelon ends up being used by elected and bureaucratic officials to their political advantage or by the intelligence agencies themselves for the purpose of sustaining their privileged powers and bloated budgets," says Mr. Poole. "The availability of such invasive technology practically begs for abuse."

Ottawa bureaucrat Claude Hisson, the commissioner for the Communications Security Establishment, is charged with investigating any complaints into CSE operations. In his most recent annual report, he admits that, on occasion, our spies intercept private conversations. But he insists there is nothing to worry about. "The sophistication of CSE's technology has led to speculation about the organization's capability to intercept the communications of Canadians," Mr. Hisson says.

"However, I have observed that CSE's activities are driven not by the capabilities of the technology it deploys but by its mandate to fulfill the foreign intelligence requirements established by the Government of Canada. ... In keeping with the policy of the government, CSE goes to considerable effort to avoid collecting Canadian communications."

Still, critics of Echelon warn the potential for abuse never goes away.

"This whole thing is so bizarrely powerful that the opportunity or

temptation

for abuse is fairly substantial," says Mr. Pike of the American Federation of

Scientists. "How many people in your organization always obey the rules?

"The notion that NSA or any other of these spy networks is the only large organization in human history in which everyone always obeys the rules just flies in the face of common sense," he says

*

* NOTE: In accordance with Title 17 <U.S.C.> Section 107, this material is

* distributed without profit or payment to those who have expressed a

* prior interest in receiving this information for non-profit research and

* educational purposes only. Provided by G2-Forward.

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: allan berg <bergax@cs.jmu.edu> (allan berg <bergax@cs.jmu.edu> [UNKNOWN]

CREATION DATE/TIME: 6-MAR-2000 16:54:25.00

SUBJECT: (ai) Desperately Seeking Signals (Text) (fwd)

TO: Mark C. Montgomery (CN=Mark C. Montgomery/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TO: Jeffrey A. Hunker (CN=Jeffrey A. Hunker/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TEXT:

Allan Berg
Director, INFOSEC Program Office
bergax@jmu.edu
O) 540.568.8773
F) 540.568.6023
WWW.INFOSEC.JMU.EDU

----- Forwarded message -----

Date: Mon, 6 Mar 2000 09:13:14 EST

From: WILSONGI@aol.com

To: ACCESS@g2-forward.org, nipmail@xmission.com

Subject: (ai) Desperately Seeking Signals (Text)

<http://www.bullatomsci.org/issues/2000/ma00/ma00richelson.html>

March/April 2000

Vol. 56, No. 2, pp. 47-51

Bulletin of Atomic Scientists

Desperately Seeking Signals
by Jeffrey Richelson

The fear that "big brother" might be monitoring our private communications is not new. It's no wonder that when a January 1998 report to the European Parliament, An Appraisal of Technologies of Political Control, claimed that "within Europe, all e-mail, telephone, and fax communications are routinely intercepted by the United States National Security Agency, transferring all target information from the European mainland . . . to Fort Meade in Maryland," it triggered a political controversy that continues to this day. The study also asserted that the key to the eavesdropping operation was a system code-named "Echelon," designed to indiscriminately intercept the non-military communications of governments, private organizations, and businesses on behalf of the United States and its primary partners in the decades-old UKUSA signals intelligence alliance--Britain, Australia, Canada, and New Zealand. Items of intelligence value are selected by computer identification of keywords provided by the UKUSA nations.

In response to extensive press coverage across Europe, the European Parliament commissioned a second report that focused exclusively on Echelon and communications intelligence. Sweden's foreign minister promised to investigate whether Swedish companies were harmed by U.S. spying. Last October, activists on both sides of the Atlantic participated in "Jam Echelon

Day" by sending a high volume of communications containing words, such as "terrorism," which they expected to be on the keyword list, in hopes of overloading the system.

The Australian and New Zealand public have also taken an interest. And in the United States, the conservative Free Congress Foundation issued a report on the topic titled Echelon: America's Secret Global Surveillance Network. The American Civil Liberties Union maintains an "Echelon Watch" section on its web site, at www.aclu.org/echelonwatch. The controversy has even reached into the halls of Congress, where Cong. Porter Goss of Florida, the Republican chair of the House Permanent Select Committee on Intelligence, requested that the National Security Agency (NSA) provide internal documents that would help reassure the committee that U.S. signals intelligence activities are not violating the privacy rights of Americans. Meanwhile, at the instigation of Republican Cong. Bob Barr of Georgia, hearings are scheduled for the current session of Congress to explore that issue.

The fear, press coverage, and rhetoric surrounding Echelon begs the question: could this be a case where life is imitating art? A number of recent films (Sneakers, Enemy of the State, Mercury Rising, The Shadow Conspiracy) depict the NSA as an organization that ignores legal restraints in pursuit of its vision of national security (and career advancement for key personnel). It is possible that some of the reporting and oratory concerning Echelon may be as over-the-top as these films, in which NSA officials also casually authorize murder, even of small children.

The Echelon network

That the UKUSA alliance, particularly as a result of U.S. efforts, operates an electronic eavesdropping network with global reach should come as no surprise. The National Reconnaissance Office maintains a constellation of geosynchronous, elliptically orbiting, and low-earth orbiting satellites that intercept communications, missile telemetry, and radar emanations. Civilian and military personnel run satellite ground stations in Britain, Germany, Australia, and Colorado which control the satellites and receive the intercepted signals. The Air Combat Command and the navy fly a variety of planes equipped to scoop up communications and other electronic signals. Nor has the end of the Cold War led to the termination of ship-based signals intelligence collection or submarine reconnaissance operations--including operations to tap undersea cables.

Ground intercept sites also continue to be part of the eavesdropping network.

While the United States closed down a number of stations in the aftermath of the Cold War--particularly those that intercepted high-frequency military communications--ground sites still form an important part of the UKUSA network. One particular set of ground stations is devoted to the interception of satellite communications--or the "COMSAT intercept mission."

According to much of the press coverage, Echelon is the code word for the

UKUSA "global surveillance network." But it is not, nor is there any code word for the overall U.S. or UKUSA "SIGINT (Signals Intelligence) apparatus. Rather, the U.S. system is known as the United States Sigint System (USSS).

Echelon is, however, very real. Its existence was first revealed by British investigative reporter Duncan Campbell in an August 12, 1988 New Statesman article. In 1996, New Zealand peace activist Nicky Hager provided a detailed description of the program in his book, *Secret Power: New Zealand's Role in the International Spy Network*, an extraordinary examination of New Zealand's SIGINT agency and its place in the UKUSA alliance. Virtually all reporting, including the original report to the European Parliament, is derived from these works. Unfortunately, much of the reporting does not accurately reflect what Campbell and Hager wrote.

The Echelon system that Hager describes links together computers, known as "dictionaries," at UKUSA ground stations. Those computers contain, for each of the cooperating agencies, a list of keywords whose appearance in any intercepted message makes the message an item of interest to the agency. The computers automatically search through millions of intercepted messages for the ones containing the pre-programmed keywords and then ship the selected messages off to the computers of the requesting agency.

Before Echelon appeared in the 1970s, the agencies shared intelligence, but they usually processed and analyzed the intercepted communications. As a result, most exchanges involved finished reports rather than raw intercepts.

Echelon, on the other hand, is an integrated network that allows the agencies to specify which intercepts are of interest and to receive them automatically via computer. A key question, then, is which UKUSA ground stations are part of the Echelon network?

COMSAT intercept sites are clearly part of that network. Almost 20 years ago, author James Bamford revealed in *The Puzzle Palace* that NSA-operated antennas at Sugar Grove, West Virginia, and Yakima, Washington, targeted the signals to and from INTELSAT communications satellites. Just 60 miles from Sugar Grove, at Etam, West Virginia, telephone calls, telegrams, and telexes arriving from or destined for 134 countries passed through an array of satellite dishes. The NSA operation at the obscure Yakima Firing Range, Bamford reported, was conveniently located 100 miles south of a similar station in north-central Washington.

Photo courtesy Duncan Campbell

Antennas at Sugar Grove, West Virginia, monitor COMSAT and INTELSAT traffic.

Today, Sugar Grove hosts both navy and air force SIGINT units that operate four satellite antennas targeted on the communications flowing in and out of the Etam ground station. The mission of the air force unit was described in the 1998-99 Air Intelligence Agency Almanac as providing "enhanced intelligence support to air force operational commanders and other consumers of COMSAT information." That Sugar Grove is part of the Echelon program is clear from declassified Naval Security Group Command regulation C5450.48A, which notes that one of the duties of Sugar Grove's commander is to "maintain and operate an Echelon site."

The air force unit at Sugar Grove is a detachment of the Air Intelligence Agency's 544th Intelligence Group; Yakima and Sabana Seca, Puerto Rico (another COMSAT intercept site), host detachments from the 544th IG, evidence that they are also part of the Echelon network. More evidence is provided by the official History of the Air Intelligence Agency (AIA) for 1994, which contains a section titled "Activation of Echelon Units." That section noted that, in 1994, the AIA, NSA, and the navy's SIGINT agency "drafted agreements to increase AIA participation in the growing [deleted, but apparently 'civilian communications'] mission" and that AIA was to establish detachments of the 544th Intelligence Group to accomplish that objective.

The other partners to the UKUSA agreement do not have the resources or incentive to maintain an array of SIGINT systems similar to those of the United States. But they can and do operate COMSAT intercept sites. Even tiny New Zealand has a modern intercept facility on its east coast at Waihopai. Hager reports that the station, operational since 1989, consists of a services building, two satellite dishes under large radomes, and an operations building. If there was any doubt about what was going on at the facility, it was dispelled when a television reporter entered the station and filmed close-ups of INTELSAT technical manuals held in the control center, as Duncan Campbell wrote in his 1999 report to the European Parliament, *Interception Capabilities 2000*.

Meanwhile, Australia operates a more extensive intercept facility at Geraldton in western Australia. When Geraldton opened in 1993 it had four intercept dishes targeted on INTELSATs orbiting above the Indian Ocean and Pacific. Among the keywords in the Geraldton dictionary are ones related to North Korea's economic, diplomatic, and military situation, Japanese trade ministry plans, and developments in Pakistani nuclear weapons technology. Another Australian intercept site, at Shoal Bay on the northern-central coast, began operating in late 1979, with two dishes targeted on Indonesian communications satellites. Shoal Bay is not, however, part of the Echelon network, as Australia refuses to share the raw intercepts with the United States and Britain.¹

The other UKUSA partners also target communications satellites. A Canadian Communications Security Establishment site at Leitrim appears to intercept the signals from communications satellites over Latin America. Britain's Government Communications Headquarters operates a major COMSAT intercept site

at Morwenstow, near Bude, Cornwall.2

While Echelon's dictionary computers are also present at the ground stations for U.S. SIGINT satellites, the stations do not appear to be tied into the Echelon network. According to Campbell, they sort through intercepted material in the same way that the Echelon dictionaries do, but their intercepts are not made available to U.S. partners. Nor do any cable tapping operations appear to feed into Echelon.

Chinks in the armor

That "Echelon" is not synonymous with the entire UKUSA eavesdropping effort does not mean that the questions raised about it are not valid. An intercept operation that scoops up a good deal of the world's communications satellite traffic, automatically processes it in search of whatever intelligence any UKUSA nation wished, and then sends it on its way, would be unsettling.

At least for the immediate future the reality seems to be somewhat less frightening. The UKUSA SIGINT agencies certainly do not intercept every signal that passes through the airwaves. And, because of the volume of communications, the expense of collection systems, and the limits of their computer resources, NSA and its allies have always had to prioritize targets and selectively task collection systems. Campbell notes in *Interception Capabilities* that it is possible to identify certain satellite signals, whether television or communications, as of no intelligence interest, and that "these signals will not progress further within the system."

There is also a significant limit imposed on the ability to monitor voice communications, resulting from the failure of extensive U.S. efforts to produce "word spotting" software that would allow computer transcription of intercepted conversations. In 1993, former NSA director Bobby Inman admitted that "I have wasted more U.S. taxpayer dollars trying to do that [word spotting in speech] than anything else in my intelligence career." Nor has the capability been developed in the intervening years, according to Campbell's report.

Thus, while faxes, telexes, e-mail, and computer traffic are subject to automatic processing and analysis, phone calls are not--although the phones of the parties involved in a call can be automatically identified and voice-prints can be used to identify who is speaking.

Congressional intelligence oversight committees have recently lambasted NSA for its failure to adequately modernize its operations. Last year, the House Permanent Select Committee on Intelligence (HPSCI) stated that as result of NSA's failure to address process and management problems, "The committee believes that NSA is in serious trouble." Later that year, Cong. Sanford Bishop Jr., a Democrat from Georgia, said that although NSA is facing "tremendous challenges coping with the explosive development of commercial communications and computer technology . . . [the agency] has not demonstrated much prowess in coping with the challenge."

A year earlier, on October 5, 1998, HPSCI Staff Director John Millis told the Central Intelligence Retirees Association, "Signals intelligence is in a crisis. . . . In the past four or five years technology has moved from being the friend to being the enemy of SIGINT." Millis went on to suggest that the United States "shouldn't be spending one more dollar than we do to try and intercept communications . . . from space."

That judgment is reinforced by a number of articles, the most prominent one by investigative journalist Seymour Hersh in the December 6, 1999 New Yorker, which have painted a picture of NSA as an organization facing serious challenges. At least three developments have reduced NSA's ability to collect and process communications.

One is the expanding use of fiber-optic cables. Any signal sent through the air can be snatched out of the air, but signals transmitted on fiber optic cannot. Tapping them has also apparently proven a major challenge in ways that tapping conventional cables has not, according to Campbell's report.

A second problem is the quantum leap in the sophistication of encryption software. A September 16, 1999 cabinet-level report to President Clinton noted that recipient can unscramble the message and read the original plain text, unless someone else has gained access to the corresponding decoding software and decryption key."

The explosion in communications volume, because of the widespread use of cell phones, faxes, and the Internet, is also a problem. As communications increase, the percentage of messages containing valuable intelligence drops, and finding that information becomes more and more difficult. Hersh reports that daily satellite telephone calls in the Arab world, many of which are encrypted, number in the millions.

Checks and balances

Even if it becomes widely accepted that Echelon is not a technological Big Brother, individuals across the political spectrum are likely to remain concerned about violations of individual privacy. The NSA and its allies clearly do intercept an enormous volume of data. And a breakthrough in word-spotting or other technologies that would allow upgrades to Echelon certainly cannot be ruled out. In addition, many have not forgotten NSA's role in monitoring the activities of dissidents during the Vietnam War, which

Bob Woodward disclosed in the October 13, 1975 Washington Post. And Hager revealed that in the past Britain's Government Communication Headquarters gathered communications intelligence on Amnesty International, apparently through the Echelon network.

The recent controversy over Echelon has led both Australian and Canadian authorities to issue unprecedented statements--acknowledging for the first time their participation in the UKUSA alliance and stating that precautions

are being taken to safeguard the privacy of their own citizens as well as those of the other UKUSA nations.

In a letter to the Australian news program Sunday Nine, Martin Brady, director of the Defense Signals Directorate, revealed the existence of a classified directive, "Rules on SIGINT and Australian Persons." The directive, with certain exceptions, prohibits the deliberate interception of communications between Australians in Australia, the dissemination of information on Australians gained accidentally during the course of routine collection on foreign communications, and the reporting or recording of the names of Australians mentioned in foreign communications.

In his 1997-98 report, the commissioner of the Canadian Communications Security Establishment reported that policies existed which required his employees "to conduct their operational activities in strict recognition of .

. . the rights, privacy, and freedoms of Canadians." He also noted the existence of a reciprocal agreement whose purpose was to ensure that UKUSA nations did not "circumvent their own legislation" by targeting the communications of each other's citizens by request. "They do not do indirectly what would be unlawful for them to do directly," the commissioner wrote.

The guidelines under which NSA operates require that if it incidentally obtains a communication from or to a U.S. citizen or organization in the United States for which there is no warrant or court order, the agency can retain the message but must remove the name of the citizen or company.

There

are several exceptions--for example, the name can be retained if NSA officials believe it is "necessary to understand foreign intelligence information or assess its importance" or if the intercept indicates that the individual "may be an agent of a foreign power."

Such guidance is the subject of U.S. Signals Intelligence Directive 18, "Limitations and Procedures in Signals Intelligence Operations of the USSS"--one of a number of classified directives issued by the Director of NSA

that guide the operation of U.S. Signals intelligence activities. A redacted

version from 1980 notes that the purpose of the 50-page directive is to "ensure that the SIGINT mission of the National Security Agency . . . is conducted in a manner that guarantees proper safeguards to the rights and privacy of U.S. persons." Four sections of the October 20, 1980 directive, portions of which were blacked out when the document was released in response

to a Freedom of Information Act request, concern the guidelines on the collection, processing, storage, and dissemination of the communications of U.S. citizens.

Two challenges

Evidence that these guidelines do reach down to the collectors can be found in the 1991 navy regulation concerning Sugar Grove. The commander of the site, in addition to being instructed to operate an Echelon site and to "[gather], process, and report intelligence," is ordered to "ensure the privacy of U.S. Citizens are [sic] properly safeguarded pursuant to the provisions of USSID 18."

But many, including Congs. Goss and Barr, want more reassurance than is provided by these documents. Goss requested, on behalf of the HPSCI, all legal opinions and guidance provided by NSA's legal office to NSA's operations staff and others--which could demonstrate how the agency is applying the laws that restrict their collection of information about American citizens. NSA argued that some of the documents could not be provided due to "government attorney-client privilege." Discussions between the two parties are continuing.

Further, the November 5, 1999 conference report on the intelligence authorization act directed the director of NSA, the director of Central Intelligence, and the attorney general to prepare a report, in classified and unclassified forms, providing a detailed analysis of the legal standards employed by the intelligence community in signals intelligence operations. The report is to cover standards for the acquisition of SIGINT about Americans as a result of U.S. Signals intelligence operations as well as those of U.S. allies.

In recent years, NSA has reduced some of the secrecy surrounding the agency and U.S. SIGINT operations. But it faces two challenges--providing needed intelligence in the face of new technological challenges and convincing both

critics and friends that it will do so without infringing on basic freedoms.

To do the latter it may have to open up even more.

--

Jeffrey Richelson is a senior fellow with the National Security Archive, Washington, D.C. Some documents pertaining to Echelon can be found at www.gwu.edu/~nsarchiv.

1. Desmond Ball, Australia's Secret Space Programs (Canberra: The Australian National University, 1988), pp. 5, 18, 36; Nicky Hager, Secret Power: New Zealand's Role in the International Spy Network (Nelson, N.Z.: Craig Potton, 1996), pp. 34-35; Duncan Campbell, "Careful, They Might Hear You," The Age, May 23, 1998; communication from Duncan Campbell, January 4, 2000.

2. Nicky Hager, Secret Power, p.39; Duncan Campbell, Interception Capabilities 2000 (Luxembourg: European Parliament, 1999), p. 7

*

* NOTE: In accordance with Title 17 <U.S.C.> Section 107, this material is
* distributed without profit or payment to those who have expressed a
* prior interest in receiving this information for non-profit research and
* educational purposes only. Provided by G2-Forward.

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: "Kurtz, James" <JKurtz@ida.org> ("Kurtz, James" <JKurtz@ida.org> [UNKNOWN

CREATION DATE/TIME:19-JUN-2000 07:52:49.00

SUBJECT: FW: CYBER RISKS - SECRET NO MORE

TO: Mark C. Montgomery (CN=Mark C. Montgomery/OU=NSC/O=EOP [NSC])
READ:UNKNOWN

TO: Jeffrey A. Hunker (CN=Jeffrey A. Hunker/OU=NSC/O=EOP [NSC])
READ:UNKNOWN

TEXT:

-----Original Message-----

SECRET NO MORE

The Hazards and Vulnerabilities of the Digital Age

With the evolution of electronic communications the Gilded Age of secrecy and sub rosa is all but over. It is harder and harder to keep secrets secret. Security is somewhat a misnomer now. The White House leaks; the State Department is losing its statecraft; CIA's private world is almost public; and the "Puzzle Palace" (National Security Agency) is downright puzzled. Our dependence on the digital age jeopardizes our national security and our right to privacy. This paper examines the problems and proposes some possible answers; please keep in mind that simplification is adopted, whenever possible, to interpret the complex details of this subject, and that the author is not an expert in the field of data processing.

One can't write about the loss of secrecy without mentioning Echelon, the Cold War surveillance system that is still in existence. This array of "ears" that spans the globe, is part of the UKUSA intelligence alliance and consists of deep space satellites and intercept stations that receive all communications, whether cellular, microwave, fiber-optic or satellite and processed by powerful computers that are programmed to pick up key words and phrases, suspect address and specific individuals voices. Certain non-member European countries have recently protested that the system is being abused and used for economic espionage. Their complaints are hard to take seriously as many of these countries have extensive electronic espionage networks of their own which are put to a good deal of questionable use.

For example, the Clinton Administration, which never took security very seriously from the outset, recently found that White House, State Department and other high-level government offices communications systems were thoroughly compromised by the Israelis. Worse, Israel's clandestine intrusions might have been picked up a lot sooner had the administration been more serious about security procedures and if Attorney General, Janet Reno had not been reluctant to seek an indictment against a suspect, an Israeli businessman working for the DC phone company. The FBI had been tracking him and his wife for over a year and was pretty certain she was a Mossad agent under diplomatic cover at the Israeli Washington, DC embassy. The FBI investigation found her husband had even penetrated the Bureau's telephone system, including the most secret and sensitive communications, even those involving this highly classified counterespionage operation. Besides lax telephone security procedures in the White House, (many people just don't bother

using a secure line), the key to the intrusion against the White House supposedly secure \$30 million computerized communication system, appears to be the software installed by the local telephone company for their billing process. It was this software, which was connected to the White House database link, that was used to access classified and regular communications. Another technical security lapse, unearthed during the investigation, was the fortuitous discovery that the "electronic back door" used by technicians to service the system, had been left wide open.

The fact that some parts of telecommunication information, such as "secret" phone numbers, trunk lines, remote sites and passwords are accessible to anyone with some computer knowledge is a major security hazard. Spies, with a detailed knowledge of computer codes that are used to route telephone traffic, pose a grave security risk since these software codes are a means of access that enables conversations to be monitored and even remotely transcribed to another location - as was the case involving our government's communications system.

As an example of the security issues we are confronted with, a pair of Israeli mathematicians, Eli Biham and Adi Shamir, have discovered a code-breaking method that only needs a simple desktop computer and a microwave generator. They call it Differential Fault Analysis (DFA). Their technique is effective no matter how long the secret prime number "keys", used to encrypt data, happens to be and it doesn't even require knowledge of what system is being used to encrypt. It is based on the study that microwaves can subtly corrupt the data stored in a micro chip and incite it to make errors in encrypting information. The errors are the means of revealing the secret of the key system used. It has been well demonstrated by a team of computer and encryption experts that this odd, new technique can break virtually any code system, including Data Encryption Standard (DES) the system most employed in the world. Furthermore, the same encryption attack can even break triple DES which, with its 168 bits of key, was thought to be unbreakable. Moreover, this can be done without an overload of text or a massive amount of computers.

Here is how it works: An encryption device encrypts the original text, then the same text is fed into the device again, but this time the device is exposed to a burst of electromagnetic radiation, i.e.: microwaves from a high-frequency radio transmitter. This activates random errors in the circuitry storing the secret keys. The process is repeated several times giving a series of encrypted messages, each one produced by progressively corrupted numerical keys. Then, by using an ordinary PC to compare the messages with the original, one can figure out the form of the original key, which once discovered, can be fed into a computer simulation of the encryption system which in turn reveals the content of the message.

Kill the messenger. Human beings are the weak link in the computer and communication security chain. They often describe the security measure taken for all to hear, and being the ones that program the systems, hold the ultimate master key to their secrets systems. We tend to put our confidence blindly into a subject just to get what we think is the consummate solution to a difficult problem, and damn the consequences. The quintessential example would be the former major in the KGB, Victor Sheymov, who defected 20 years ago and went to work for NSA trying to find techniques to break into the KGB communication systems he had designed. Eventually he left the government agency because of a dispute over money that he insisted was owed to him by the US Government as part of the defection agreement he had accepted. He then worked up a set of

programming instructions based on his own algorithm procedure, which he claims makes any machine hacker-proof. His former NSA colleagues supposedly tested his invention and found the system impregnable. He is now the owner of his own cyber security company outside Washington, DC and government offices are interested in his discovery. Of course the vulnerability of the security system Mr Sheymov invented lies in the integrity of the man.

It isn't only systems that are vulnerable, so are the very machines that house the systems. Spies can reassemble what is written on a computer by interpreting the intercepted radio-frequency emissions from the computer's electronics. Electronic keyboards are susceptible to eavesdropping because they rely on a scanning signal that radiates the pattern of keys being used. And a new system has been developed in the United States that allows someone to access any file on the hard drive of a targeted computer and record every key stroke made on it. It also allows someone to read any encrypted message regardless of the encryption used in near real time. Such surveillance technology makes it possible for law enforcement agencies (or criminals and spies) to remotely monitor a PC anywhere on the globe and stealthy transmit the data back to a pre-determined covert internet address monitored and decoded by the operating system. Rather than physically having to place a chip surreptitiously inside a targeted computer, this new method allows one to monitor the computer electronically by placing covert software via the Internet into the PC.

It is an exaggeration to conclude that modern technology has revolutionized clandestine terrorist activity, aided the criminals and made our world all the more secure. For them to use encryption is a dead giveaway. Routine NSA monitoring would pick out the encrypted traffic and would flag the phone number for further monitoring. Encryption, instead of increasing one's security, lessens it. It is back to basics for the criminal world. For example, an ordinary cigarette paper is used to transmit information and orders from one criminal cell to another. The paper is wrapped in plain kitchen plastic wrap and the courier transports the message concealed in his mouth.

While prepaid card cell phones are anonymous and untraceable, making them useful for running illegal operations, such as drug dealing, they still can be easily tapped. And security agencies (or spies) can eavesdrop on conventional cell phone users by setting up a monitor station at the exchange where cell phone calls are connected to fixed public phones via gateways, networks, and simply tap into the link. The future harbors further risks. The new breed of "intelligent" programmable cell phones will be open to hacking and espionage like our computers are today. A virus could be easily introduced via the built-in programs, record conversations and pass them on to another phone.

Modern criminals use active scanners which have an approximate radius range of about 1 km. (actually only a modified cell phone that simulates a phone networks base station) to hack into another cell phone. The criminal stations himself in a busy place such as an airport to tap into the control channel of a cell phone and within minutes can covertly identify the numbers of legitimate cell phones to then clone to his stolen cell phone. It is simpler than one would think because of the way cell phones operate. Cell phone systems constantly check the location of every cell phone in operation, so that incoming calls can be routed to the legitimate phone. This is done by a base station that sends out signals (a pair of numbers) "asking" every phone in use to reply with its number pair. All the criminal or spy has to do is to mimic this method and all the cell phones in the proximity will respond with their

pair numbers. The bogus base station is connected to a conventional PC which builds a database of number pairs until a match pair is captured, usually within a matter of minutes.

Our criminal or spy can also opt for a device called a dongle, if he wants to splurge about \$150. The gismo isn't any larger than a large coin and plugs directly into the cell phone socket used for servicing purposes. This socket contains the chip that stores the control software. Once the dongle is plugged into the socket anyone can manipulate the stolen phone into a clone of a legitimate one, simply by keying in a new identity number on the phone's keyboard. To counter stolen cell phones, a new generation of phones have a chip incorporated in them that makes them act like a microphone, allowing someone to receive your conversations and trail your movements. Even after being turned off, the system works for a while, taking its power from the cell phones battery. Ironically, cloned phones and prepaid ones are probably the only secure phones around today; at least the caller's identity can be kept secret even if his location can be known.

You are not only being overheard, you are being increasingly watched by high-tech hidden surveillance cameras that actually do more than just film you. People's ordinary behavior is surprisingly alike, almost mathematically predictable. A new generation of computers have been programmed to spot deviate patterns that imply criminal activity, focus in on the subject and record on film the criminal act, such as planting a bomb, stealing a car or picking someone's pocket. In the future, an array of cameras on the street and in public buildings, tuned to your gestures, gait and facial recognition (called threshold values in computerspeak) will be able to follow your every move. Comforting thought.

So where is this invasion of privacy leading us to? Ironically, not to more security but to diminished security. It is increasingly more difficult to safeguard our own security secrets because clandestine intrusions have gained the upper hand. Something has to be done to redress the situation.

Trying to build leak-proof firewalls, safe areas protected by codes and protocols that are hacker resistant doesn't seem to be the way forward. As we have seen, codes can be unlocked and firewalls can be by-passed and protocols can be corrupted. Rather than trying to fence off areas to a computer attack, an in-depth defense, made up of several layers and lying in ambush for an intruder, might prove more efficient. The countermeasures would begin once an intruder has broken into the system; he could be given false data from bogus files or be ensnared by a virus that would counter-attack the intruder. Sensitive files could be camouflaged behind phony codes and hidden in unlikely, pedestrian places. A new breed of hypersensitive microchips used in quantum cryptography could help in securing optic-fiber communications. Scientists have discovered how to detect a single photon using this new chip. They argue that if an encryption key is superimposed on a single photon, any hacker intercepting the photon in an optical-fiber communication would alter its quantum state, alerting the receiver to the interception, who could then change the key. Another principal liability, and the vectors of electronic viruses, are the programmable devices that have a link to one another. Modern phones with built-in programs should have their programs separated so that one program can't self-start another one. If the virus can't get out of the program it can not be spread elsewhere. Some experts think the future is in mathematical proofs that confirm when a system is secure. The dilemma is that people want more functions and ease of operation built into their

communications systems but not the liability of viruses and eavesdropping that goes with it. A choice has to be made; it doesn't look like we can have both. Security or insecurity.

Peter B. Martin
June 2000

*NOTE: In accordance with Title 17 <U.S.C.> Section 107, this material
* is distributed without profit or payment to those who have expressed a
* prior interest in receiving this information for non-profit research and
* educational purposes only.

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: allan berg <bergax@cs.jmu.edu> (allan berg <bergax@cs.jmu.edu> [UNKNOWN]

CREATION DATE/TIME: 5-JUL-2000 17:19:42.00

SUBJECT: (ai) Loeb - Chat Transcripts on Intelligence Issues (fwd)

TO: "Undisclosed.recipients:;"@eop.gov ("Undisclosed.recipients:;"@eop.gov [UNKNOWN
READ:UNKNOWN

Mark C. Montgomery (CN=Mark C. Montgomery/OU=NSC/O=EOP [NSC])
READ:UNKNOWN

TEXT:

Allan Berg
Director, INFOSEC Program Office
bergax@jmu.edu
O) 540.568.8773
F) 540.568.6023
WWW.INFOSEC.JMU.EDU

----- Forwarded message -----

Date: Wed, 5 Jul 2000 14:25:59 -0400
From: "Forno, Rick" <rforo@netsol.com>
To: 'access' <access@g2-forward.org>
Subject: (ai) Loeb - Chat Transcripts on Intelligence Issues

Back Channels With Vernon Loeb

Wednesday, July 5, 2000 1 p.m. EDT

Washington Post reporter Vernon Loeb covers national security issues. In his latest articles, Loeb focuses on allegations that Wen Ho Lee was prosecuted for spying on the basis of his race; the Discoverer II satellite program and the dispute over a forthcoming book by former CIA operative Bob Baer.

Gainesville, Florida: Is it reasonable to assume that Wen Ho Lee was the ONLY person removing secrets from the lab? Is it likely that others did so as well and Wen Ho Lee did not but got the blame?

Vernon Loeb: It is certainly possible that other scientists at Los Alamos were removing secrets and didn't get caught. But I think it's easy to get carried away with such speculation. In my opinion, the vast majority of scientists at Los Alamos and the other weapons labs have been, and are, very careful in their handling of secret information. I do not see Los Alamos, Livermore and Sandia as facilities brimming with spies, by any means.

Tallahassee, Florida: What happened to the N.Y. Times reporter who first reported on Lee? I have not seen him writing articles for a long time.
Vernon Loeb: You got me on that one.

slingerlands, NY: Since the Computer Security act of 1987 clearly requires the government to implement levels of security exceeding a B-2 level for data such as that found on Mr. Lee's home and unclassified system, why is he, and many other people saying he did nothing wrong?
Does DOE just ignore the legally required protections of our most sensitive data?

Vernon Loeb: I haven't encountered anyone who is saying Wen Ho Lee did nothing wrong. Virtually everyone, with the possible exception of Lee's lawyers, concede that he seems to have committed major violations of

existing lab and DOE computer security regulations. Whether what he did constitutes a violation of the Atomic Energy Act and Espionage Act are the key questions before the court.

New Orleans, LA: In connection with the missing computers at State and the bug found there, are our efforts at security inept?

Vernon Loeb: I think it's an over simplification to say that the U.S. government's security efforts are inept. I think the evidence suggests that there was some laxity about security in certain quarters of the State Department and Energy Department. But I do not believe the national labs are

the sieves that their detractors in congress describe. And I do not believe that security in the State Department is anywhere near as bad as the detractors claim. Were there problems? There seem to have been. But don't discount the political motivation coloring the nature of this debate. And remember, Russian intelligence is pretty good. It's quite possible for Russian spies to plant a bug inside an agency with even the best security. It's possible for them to do it. It's possible for us to do it. I

personally

think the interests of national security would be better served if the debate about legitimate security concerns were not so highly politicized.

Brooklyn, NY: According to a recent article, the CIA is recruiting more native foreign-language speakers. How does this jibe with racial profiling used by counterintel (i.e. Wen Ho Lee)? Are they setting up new recruits for failure?

Vernon Loeb: Interesting question. Clearly, the CIA's recent hiring of officers with native speaking abilities whose families may have recently emigrated to the country will pose new counterintelligence challenges. And many of them, as you suggest, will probably find out that they are subject to particular counterintelligence scrutiny. Whether this ends up ruining their careers depends upon how the agency carries out its CI mission. When questioned on this point, CIA officials say CI considerations should not be impediments to hiring recent emigres, and should not be impediments to their careers. I guess time will tell.

Ottawa, Canada: What is the federal government doing to protect its laptops and portable equipment from unauthorized access?

Vernon Loeb: There's been talk very recently of starting to encrypt everything on portable devices, which seems to make a good deal of sense to me. Clearly, laptops and other portable media like tapes and discs are things the government is only just now beginning to think about in security terms. However, there are lots of restrictions about transferring data from non-portable systems, to portable ones. So, theoretically, in any case, there shouldn't be a lot of top secret codeword information floating around out there on portable machines.

Reston, VA: What is your reaction to David Ignatius' recent column in which he took to task journalists who trade in leaked information?

Vernon Loeb: The column you're referring to was a piece David wrote about Bill Gertz, The Washington Times national security writer who is often leaked top secret documents by his sources in the intelligence community of Pentagon. I'm not sure David went so far as to take him to task. He simply posed the question, are there instances in which Gertz hurts national security by publishing classified information that has the result of shutting down, say, a signals intelligence channel. I don't know what Gertz's standards are in deciding whether to publish classified information.

The Washington Post reserves the right to publish classified information, on the belief that much government information is over-classified, but also, as a matter of policy, does weigh the concerns of U.S. intelligence officials in deciding what to publish and what not to publish. I personally I have seen instances in which we agreed not to publish classified information after U.S. officials argued that publication could harm national security or endanger the life of an intelligence source.

Carbon Cliff, Illinois: Former spooks who speak out seem to become an endangered species. What is the real story behind John Millis?
Vernon Loeb: I'm not sure I know the entire real story. Millis, the late staff director of the House Permanent Select Committee of Intelligence, had been placed on administrative leave with pay at some point, and for some duration, prior to his suicide last month. I have been assured by Rep. Porter J. Goss (R-Fla.), the committee's chairman, that the disciplinary action behind Millis' leave had nothing to do with national security, the CIA, or any other aspect of his work of interest to the public. I have also been assured that Millis was not under any type of criminal investigation.

New York, NY: CIA has recently come under considerable criticism for having become too "risk averse" in its efforts to recruit potential sources. Have any internal reviews or policy changes been implemented to address these criticisms?

Vernon Loeb: No, in fact, in responding to the "risk averse" conclusion of the National Commission of Terrorism, CIA officials pointedly disagreed and said they did not plan to rescind the regulation in question that requires the recruitment of assets with criminal records to be reviewed and approved at headquarters by the deputy director for operations. The commission concluded that that regulation has had the effect of making case officers in the field risk averse. CIA officials say it has the opposite effect, protecting field officers in recruiting criminal sources by making higher-ups at CIA headquarters sign off in the process. And that is pretty much where the debate remains.

Stevens City, VA: The July 2nd Post carried an article on the continued threat posed by Osama Bin Laden. However, an article in the New Yorker last Spring detailed how U.S. intelligence had vastly overrated Bin Laden's capabilities. What's the truth?

Vernon Loeb: I don't think the two are mutually exclusive, and I'm not sure the two articles you cite necessarily are in conflict. In fact, the July 2 post article, which I wrote, quotes a Middle East scholar as making the point that the U.S. government has overrated bin Laden's capabilities. I personally feel that bin Laden remains a threat, and that the extent of that threat is now overstated, partly because the CIA, the FBI and, more importantly, all of their overseas liaison partners, have brought a lot of pressure to bear on bin Laden's network since the embassy bombings in East Africa in August 1998.

Buffalo, New York: Do you think that S.2507 [the Intelligence Authorization Act for Fiscal Year 2001], if passed, will dampen the possibility of bureaucrats' leaking information in the future? If so, would it show, as the

Pentagon Papers did, that the US government acted and thought differently from its public statements? Keep up the good work.

Vernon Loeb: Yes, if the anti-leak provision in the intelligence

authorization act becomes law, I most certainly do think it would have a dampening effect on leaks. I also think it would be challenged and declared unconstitutional. For that reason, I do not think it will pass in its current form. But no, if passed, I think it would make it harder for the public to discern differences between what the government says, and what its classified studies sometimes say, since the risks involved in making such information public would suddenly become much greater than they are now. My personal opinion: most leaks do little or no damage to sources and methods; most leaks involve information that should not have been classified in the first place, and the leakers know that and feel free.

Middlebury, VT: Do you think the intelligence community, and the CIA in particular, get a bad rap from the press? Isn't the call for cutting their resources actually counterproductive to national security in the long run?
Vernon Loeb: I think, on balance, the CIA and the intelligence community get the rap they deserve. They get their share of blame, some of it richly deserved. They also get credit for a lot of accomplishments which they may or may not deserve credit for. As for cutting their resources, who is arguing for that? Certainly no one in Congress or the administration, and no one in the mainstream media, for that matter. Indeed, some of the harshest critics of the intelligence community that I read are in the community! I was just reading an email from a former Naval intelligence officer who was arguing that the IC is in crisis, and a former CIA case officer I know is fond of saying the IC is "too broke to fix." I think if the spy agencies themselves weren't so secretive, the media would be better able to get at some of these issues and would be better able to paint a more balanced portrait of the community's successes, and its failures.

Washington, DC: I always enjoy your columns, chats, and stories. Currently, I am reading "Black Hawk Down" on your recommendation. Along the same lines, are there any particular books you would recommend as an intelligence primer for us avid fans?

Vernon Loeb: Ted Gup's new book, The Book of Honor, is a good read about the CIA's anonymous stars. Two classics on the CIA are Thomas Powers' The Man Who Kept the Secrets, and Bob Woodward's Veil. David Ignatius' first novel, Agents of Innocence, is still my favorite spy novel and one of the best books anywhere on the ins and outs of espionage (it's based on a true story, and the work of CIA legend Robert Ames, and I'm enjoying Thomas Powers' new novel, The Confirmation. And, of course, James Bamford's The Puzzle Palace remains the definitive work on the NSA. It's now a bit dated, but Bamford is working on a sequel. That should give you enough reading to get through beach season.

VA: Will you write an article about the re-emergence of the new "KGB", especially their economic and technological spying methods?

Vernon Loeb: It's a good idea, and one I hope to get to.

Harlingen, TX: The kinds of countermeasures future enemy ICBMs will carry is currently a hot topic. Estimation of the technical characteristics of foreign weapons falls largely to the intelligence community, which is apparently preparing a National Intelligence Estimate in support of the

National Missile Defense program.

Especially since the ICBMs in question don't exist yet, the estimate will necessarily involve a fair amount of guesswork. And if past experience is an

indicator, the intelligence agencies, particularly those in the Department of Defense, will come under pressure to produce guesses/estimates pleasing to their parent organizations.

Are you seeing any signs of such pressures being applied, or any serious disagreements between DIA and CIA on the countermeasure question?

Vernon Loeb: I wish I could answer your question with any degree of sophistication, but cannot. Such inside pressures are hard for journalists like me to discern, and when they're become discernable at all, political spin often makes it hard to know what exactly is going on. I can note, however, that the LA Times recently had a good article on CIA analysts reacting skeptically on the question of the NMD program. And it's certainly not illogical to think that ideological differences could emerge between DIA

and CIA. Indeed, some of the hardliners in Congress on China have taken to attacking some of the CIA's most knowledgeable China analysts as liberals, which is a strange turn of events.

Ashburn, VA: You always seem to have some insight or inside information on the intelligence community. Knowing you won't reveal your sources, I'm left wondering if you ever worked for the Intelligence apparatus of the United States?

Vernon Loeb: Never did. I used to cover Marion Barry.

Washington, D.C.: A while back, you wrote about the guy in the tweed jacket who walked in the secretaries' office next to Secretary Albright who just helped himself to classified documents and walked out. Why were there no composite sketches made? Were the two secretaries threatened if they helped the FBI?

Vernon Loeb: I never saw any composite sketch. The man in the brown tweed coat remains an enduring mystery.

Reston, VA: You said that the federal government is planning to encrypt data

on laptops to protect the information contained on them. Doesn't this provide a false sense of security since all encryption can be broken given enough time and computing power?

Vernon Loeb: I'm not sure I know enough about encryption to answer your question. Can all encryption sooner or later be broken?

Washington, DC: Backing up a couple of months to your Intelligence quiz based on the Lowenthal book -- when did we start spying on New Zealand? I thought it -- along with the UK, Canada, Australia, and the US -- made up the so-called UKUSA countries which cooperate closely under a 1947 agreement.

Vernon Loeb: I think there may have been some rift with New Zealand back in the Reagan check with Lowenthal on that.

Harlingen, TX: Has it been established that Dr. Lee took classified or PARD data home? I had only heard that he had taken it as far as his office in LANL.

Also, has it been disclosed what kind of Internet access his office computer had?

Vernon Loeb: I don't think it's been established that Lee took anything home. In fact, in the search of his home, I don't think any PARD of classified information was found. Having said that, it's not clear where

Lee

took the seven missing tapes. Until he clears up that mystery, I will be hard to know what Lee did with the data he downloaded.

Minneapolis: Is it possible that Wen Ho Lee passed information on American strategic weapons to Taiwan, not China?

Vernon Loeb: Yes, that's possible. In fact, Lee's lawyers recently asked a federal judge to order the government to state which country they believed Lee was spying for, China, Taiwan, or somebody else. The government is supposed to have an answer by this week. There is no evidence, to date, that

Lee gave any of the information he downloaded to anyone, and most recently, the government's lawyers argued that he may have been downloading it on speculation to help him market his services to some foreign country or lab, were he to lose his job.

Albuquerque, NM: Many of the issues around the Wen Ho Lee case involve the technical significance of the material he allegedly compromised. Some of our

FBI investigators don't seem to know the difference between a nuclear secret

and the square root of two. What access does the FBI have to unbiased technical expertise needed to evaluate the consequences of Wen Ho Lee's infractions?

Vernon Loeb: The FBI certainly has access to scientists at Los Alamos. Whether or not they are unbiased is another matter. But the question you pose will be a fundamental one at Wen Ho Lee's trial_just how valuable was the information he downloaded?

Washington, DC: I am an Asian American, one of many Asian Americans who believes that Mr. Wen Ho Lee was unfairly targeted and investigated without clear and adequate basis. My question is what are the facts behind the allegation that Mr. Lee's wife was working for the U.S. government and reporting on Chinese activities?

Vernon Loeb: Mr. Lee's wife has admitted working for the FBI and informing on Chinese scientists visiting Los Alamos.

Fairfax, VA: This Wen Ho Lee thing has me caught me up for the moment. I guess the real question is why did he download so much of this TOP Secret nuclear data if he wasn't giving it to the Chinese? What was his purpose? I don't think the US government is using him as a scape goat.

Vernon Loeb: This is the enduring question of the Wen Ho Lee case. Why? Lee's defenders say he that he downloaded the information when threatened with the loss of his job back in 1992, so that he could maintain access to codes he'd spent his life working on. If Lee is to work out a plea, or prevail at trial, he's going to have to explain himself a little bit better than he has thus far.

Tulsa, OK: A French prosecutor is investigating Echelon. What is he likely to find and should some agency or court in the US be doing some investigating for us?

Vernon Loeb: I wish the French prosecutor well in his investigation of Echelon. It will be interesting to see how he chooses to proceed. I hope he asks the French whether they have any kind of SIGINT program of their own, and whether they practice industrial espionage.

Los Angeles, California: Can you please shed some light on the current situation with Echelon. What exactly is the system and its purpose? Who benefits most from the information collected?

Vernon Loeb: Echelon is merely a code name for a program by which the NSA

and its intelligence partners sort signals intelligence that is collected and search it for code names of interest. Clearly, the NSA and its partners in Britain, Australia and Canada benefit most from sharing signals intelligence, although the NSA argues that the civil liberties of U.S. entities and those of its partners are protected. We could spend an hour going over what those claimed protections are, but suffice it to say that Lt. Gen. Michael Hayden, the NSA's director, has more or less stifled the Echelon debate in the U.S., convincing Congress that his analysts scrupulously follow restrictions on eavesdropping on Americans.

Vernon Loeb: Well, we're gone a little bit past our allotted time. Thanks for all those questions. I'm sure I couldn't answer all of them. But anyone who asked a question and didn't get an answer should feel free to email me at loebv@washpost.com, and I will reply. Thanks again, and we'll do this again next month. Cheers

washingtonpost.com: Thanks to everyone for their questions. Please join us on August 16th for Vernon Loeb's next chat.

Rick Forno, Corporate Security Officer
Network Solutions, Inc.

PGP Fingerprint: 2BAE CA49 6228 3B1A 8098 3EE5 0811 9D41 3E69 4AF7

"I Have Become Comfortably Numb..."

*

* NOTE: In accordance with Title 17 <U.S.C.> Section 107, this material
* is distributed without profit or payment to those who have expressed a
* prior interest in receiving this information for non-profit research and
* educational purposes only. Provided by G2-Forward.

RECORD TYPE: FEDERAL (NOTES MAIL)

CREATOR: "Kurtz, James" <JKurtz@ida.org> ("Kurtz, James" <JKurtz@ida.org> [UNKNOWN

CREATION DATE/TIME:13-SEP-2000 14:02:01.00

SUBJECT: FW: Echelon electronic spy network

TO: Debora A. Plunkett (CN=Debora A. Plunkett/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TO: Paul B. Kurtz (CN=Paul B. Kurtz/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TO: Jeffrey A. Hunker (CN=Jeffrey A. Hunker/OU=NSC/O=EOP [NSC])

READ:UNKNOWN

TEXT:

-----Original Message-----

Wednesday, September 13 1:31 AM SGT

EU parliament seeks US congressmen on Echelon electronic spy network

BRUSSELS, Sept 12 (AFP) -

A European Parliament ad hoc committee investigating the capabilities of the

US Echelon international spy network wants to question US congressmen sitting on intelligence committees, a committee member said Tuesday.

"If it was up to me, we would invite" members of the US House and Senate involved in intelligence matters, said committee rapporteur Gerhard Schmid.

The temporary committee also said it wants to "invite" the head of the US National Security Agency, one of the most secret of US intelligence services, for questioning.

A European Parliament committee may invite officials of non-EU countries to testify, but they are under no obligation to comply.

Committee chairman Carlos Coelho said he wanted to open consultations with technical experts on October 12, and that a list of the experts would be released next week.

The ad hoc committee was set up at the beginning of July with instructions to finish its investigation on capabilities of the intelligence gathering network and report back within one year.

The US electronic surveillance system is currently under investigation by French prosecutors and is widely suspected of being deployed around the world, and particularly in Europe, as an instrument of commercial espionage.

Based at Fort Meade, Maryland, the network gathers information from listening posts stationed in the United States, Britain, Canada, Australia and New Zealand, with additional input from around 120 US satellites in geostationary orbit.

France has been angered at the loss of huge foreign contracts due to what it

believes is eavesdropping by the US National Security Agency (NSA) which it says operates the Echelon system to spy on Europe's industrial secrets through 24-hour electronic surveillance.

Paris has accused Britain of disloyalty to its European partners for allowing the Cheltenham-based GCHQ (Government Communications Headquarters) surveillance network to cooperate with Echelon, particularly at its Menwith Hill outpost where two-thirds of the 1,200 personnel are American and where, according to the Federation of American Scientists, US officials have been in control since 1966.

Echelon evolved out of the Cold War espionage system set up by the UKUSA Alliance, formed in 1948 by the United States and Britain and later joined by London's Commonwealth partners.

* NOTE: In accordance with Title 17 <U.S.C.> Section 107, this material
* is distributed without profit or payment to those who have expressed a
* prior interest in receiving this information for non-profit research and
* educational purposes only.