**Stichting Bits of Freedom**
Postbus 10746
1001 ES Amsterdam

**M** +31(0)624534440
**E** axel.arnbak@bof.nl
**W** www.bof.nl

Bankrekening 55 47 06 512
Bits of Freedom, Amsterdam
KVK-nr. 34 12 12 86

**Aan de leden van de Vaste commissie voor Justitie van de Tweede Kamer**

Betreft:
Kamerbriefing tapstatistieken

Datum:
Amsterdam, 23 november 2009

Geachte heer/mevrouw,

1. De stichting Bits of Freedom ("**Bits of Freedom**") heeft bezorgd kennis genomen van de door de Minister van Justitie gepubliceerde tapstatistieken over het jaar 2008 en de eerste helft van 2009. Gelukkig vindt op 26 november a.s. een debat hierover plaats. Met deze briefing willen wij u ondersteunen om deze zorgelijke ontwikkeling tijdens dit debat aan de kaak te stellen.

2. In deze briefing komt Bits of Freedom tot de volgende conclusies:

   - Nederland blijft ieder jaar koploper op het gebied van aftappen. Ieder jaar groeit het gemiddeld aantal dagelijks getapte lijnen, en het aantal afgeluisterde mensen neemt daardoor steeds verder toe.
   - Het Nederlandse aftapbeleid is met achteloosheid omgeven. Informatie over de effectiviteit blijft achterwege, de zorgvuldigheid laat te wensen over en de transparantie is onvoldoende.
   - Hierdoor staat het huidige aftapbeleid op gespannen voet met artikel 8 EVRM. Aan de eisen die het EHRM stelt aan aftappen, waaronder proportionaliteit en transparantie lijkt niet te worden voldaan.
   - Daarnaast brengt gebrek aan transparantie risico's met zich voor de rechtstaat.
   - Ook heeft dit gebrek aan transparantie een negatieve uitwerking op de veiligheid.

3. De Nederlandse overheid dient haar beleid fundamenteel aan te passen, zodat (i) een strenger toetsingskader wordt ontwikkeld voor het aftapbeleid, (ii) meer openheid wordt gegeven over het aftappen van telecommunicatie en (iii) eindelijk de notificatieplicht wordt nageleefd.

**Nederland blijft ieder jaar koploper aftappen**

4. Het aftappen van telecommunicatie vindt in Nederland buitengewoon vaak plaats, zoals blijkt uit de recent door de Minister gepubliceerde tapstatistieken. Ook in 2009 lijkt weer een record te worden gebroken.

> In 2008 is op meer dan 26.425 telefoonnummers een bevel tot aftappen afgegeven (de taps van de AIVD en de MIVD zijn hierin niet meegenomen). Het betrof in 90% van de gevallen een tap op een mobiele telefoon en in 10% een tap op een vaste telefoonaansluiting. Gemiddeld liepen er in 2008 dagelijks 1946 taps. Het aantal taps is bovendien significant gestegen ten opzichte van 2007. Justitie heeft in de eerste zes maanden van 2009 ruim 13.000 telefoonnummers afgeluisterd, met een gemiddelde van 2250 telefoonnummers per dag. Waar het aantal afgeluisterde telefoonnummers nog steeds bijzonder hoog ligt, is het gemiddeld aantal taps per dag met circa 16% gestegen ten opzichte van 2008.

5. Dat zijn schokkende cijfers, maar eigenlijk schetsen deze nog een te beperkt beeld, want er worden veel meer *mensen afgeluisterd dan er taps worden gezet*.

> Iedereen die naar een afgetapte lijn belt, of vanaf een afgetapte lijn wordt gebeld, wordt immers ook afgeluisterd. Daarnaast begrijpt Bits of Freedom dat ook lijnen in huizen van bewaring worden afgetapt om een aantal specifieke gedetineerden af te luisteren; hierdoor worden echter ook duizenden gevangen die *niet* voorwerp zijn van onderzoek afgeluisterd.

6. Gelet op het aantal tapbevelen dat in andere landen is afgegeven, moet worden geconcludeerd dat Nederland in relatieve zin – per hoofd van de bevolking – koploper is, en zelfs in absolute zin – cijfermatig – tot de wereldtop behoort.

> **Verenigde Staten**: 1.891 tapbevelen (2008), populatie meer dan 300 miljoen.
> **Verenigd Koninkrijk**: 1.508 tapbevelen (2008), populatie meer dan 60 miljoen.
> **Frankrijk**: 26.000 tapbevelen (2008), populatie ongeveer 65 miljoen.
> **Duitsland**: 44.000 tapbevelen (2007), populatie meer dan 80 miljoen.
> **België**: 3.603 tapbevelen (2007), populatie ongeveer 10,4 miljoen.
> **Nederland**: meer dan 26.000 tapbevelen (2008), populatie ongeveer 16 miljoen.
> Daarbij dient een aantal belangrijke kanttekeningen geplaatst te worden, die deze cijfermatige vergelijking mogelijk minder relevant maakt. Ten eerste is in sommige landen de functie van taps beperkter: zo begrijpen wij dat deze in het Verenigd Koninkrijk niet gebruikt mogen worden als bewijs, maar slechts als sturingsinformatie. Bovendien is de vraag of de manier waarop deze cijfers zijn berekend, wel hetzelfde is (het is bijvoorbeeld niet zeker dat in andere landen ook de Nederlandse maatstaf van één tap per bevel wordt gehanteerd).

**Het aftapbeleid is in Nederland met achteloosheid omgeven**

7. Tegelijkertijd geeft de Minister in zijn beantwoording nauwelijks informatie over het Nederlandse aftapbeleid en de effectiviteit daarvan, en doet hij daarbij vaak een beroep op het staatsgeheim.

8. Over de effectiviteit spreekt de Minister slechts in algemene termen, en een recent evaluatierapport van hoofdstuk 13 Telecommunicatiewet noemt hij niet. Juist in dat rapport luidde één van de de hoofdconclusies toch dat door “diverse technische en marktontwikkelingen de effectiviteit en efficiëntie van de aftapbaarheidswetgeving af[nemen]”.[1]

9. Ook wordt geen informatie over het aantal en de groei van het aftappen van internetverkeer

1 Aftapbaarheid van Telecommunicatie”, TILT/Dialogic 2005,p. 67-69.

wordt verstrekt, en wordt opnieuw een beroep op staatsgeheim gedaan.[2] Bits of Freedom ziet niet in waarom het aantal taps van internetverkeer staatsgeheim zou moeten zijn. Zo blijkt uit cijfers van de Stichting NBIP, die de taps voor een aantal kleine providers verzorgt, dat in de periode 2003 tot 2006 in totaal niet meer dan 62 eindgebruikers zijn getapt. Het is onduidelijk wat hier geheim aan zou moeten zijn. De KLPD heeft verder onlangs opgemerkt dat het op dit moment niet mogelijk is "om op geautomatiseerde wijze, betrouwbare (valide) gegevens te genereren ten aanzien van het aantal taps op internet aansluitingen", maar dat is naar Bits of Freedom begrijpt onjuist: Bits of Freedom begrijpt dat voor iedere internettap een unieke encryptiesleutel moet worden aangemaakt, die door de overheid wordt bewaard. Als dit juist zou zijn, zou het aantal encryptiesleutels een precieze indicatie geven van het aantal taps. Hoe het ook zij: het is onacceptabel dat de burger hierover in het duister tast.

10. Ook informatie over gebruik van de aftapbevoegdheid door de AIVD en de MIVD wordt niet gegeven, waarbij een beroep op het staatsgeheim wordt gedaan.[3] Dat is opmerkelijk, want in België wordt deze informatie wel verstrekt: in 2006 en 2007 werden er respectievelijk afluistermaatregelen uitgevoerd met betrekking tot acht feiten en vijf feiten."[4] Waarom kan de Nederlandse overheid die transparantie niet bieden?

**Het huidige aftapbeleid staat dan ook op gespannen voet met artikel 8 EVRM**

11. Aftappen grijpt diep in op de persoonlijke levenssfeer, zo blijkt ook uit jurisprudentie van het Europese Hof. Een inbreuk op artikel 8 lid 1 Europees Verdrag tot bescherming van de Rechten van de Mens ("**EVRM**") is volgens lid 2 alleen geoorloofd als aan strikte voorwaarden is voldaan. Zo moet een inbreuk "bij wet voorzien" en "noodzakelijk in een democratische samenleving" zijn en een "legitiem belang" dienen.[5]

> Het Europees Hof voor de Rechten van de Mens ("**EHRM**") heeft in de recente uitspraak "Liberty and others v. The United Kingdom" geoordeeld dat alleen al het bestaan van wetgeving met betrekking tot het aftappen van telecommunicatie een bedreiging voor de persoonlijke levenssfeer van alle burgers en het communicatiegeheim vormt, ongeacht of deze bevoegdheid daadwerkelijk wordt toegepast.[6] Nu de rol van telecommunicatie verandert, en met name internetverkeer steeds meer verweven is met het dagelijks leven van de Nederlandse burger en zijn de persoonlijke ontwikkeling, neemt de ernst van deze inbreuk toe.

12. In inbreuk is pas "noodzakelijk in een democratische samenleving" als deze een dringende maatschappelijke behoefte vervult,[7] en de impact van de inbreuk afgewogen wordt tegen het privacybelang van burgers.[8] Bij deze afweging zijn de effectiviteit en de subsidiariteit – waren er minder inbreukmakende alternatieven denkbaar? – van aftappen doorslaggevend. Daarbij ligt de lat voor een rechtvaardiging van een inbreuk hoger, naarmate de inbreuk groter is.[9]

2 Beantwoording Minister, p. 5.

3 Beantwoording Minister, p. 5.

4 Zie http://senate.be/www/?MIval=/Vragen/SchriftelijkeVraag&LEG=4&NR=2547&LANG=nl.

5 Het criterium "legitiem belang" behoeft geen verdere aandacht, aangezien de opsporing van ernstige strafbare feiten en de nationale veiligheid door het EHRM als zodanig wordt beschouwd.

6 Zie EHRM Liberty and others v. The United Kingdom, par. 57: "mere existence of legislation which allows a system for the secret monitoring of communications entails a threat of surveillance for all those to whom the legislation may be applied".

7 De leer van de "pressing social need", zie de uitspraak van het EHRM in de zaak Silver, par. 97.

8 Dit staat bekend als het zogenaamde "proportionaliteitsvereiste", zie het EHRM in de zaak Silver, par. 97.

9 Een uitvoerige bespreking van deze thematiek is te vinden in Jacobs & White 2006, p. 232.

Vanwege de ernst van de inbreuk van het middel aftappen, dient de overheid haar aftapbeleid uitvoerig te verantwoorden.

13. Uit jurisprudentie van het EHRM over het criterium bij “wet voorzien” blijkt dat dat de Nederlandse overheid verplicht is transparant te zijn over haar aftapbeleid. Het EHRM verplicht overheden om de gehanteerde procedures rondom het onderzoeken, gebruiken en opslaan van afgeluisterd materiaal openbaar te maken, zodat de samenleving hiervan kennis kan nemen en dit kan onderzoeken.[10]

> De voorwaarde dat een inperking “bij wet voorzien” moet zijn, valt in drie deelcriteria uiteen. Een van deze deelcriteria is de voorzienbaarheid van een inbreuk, wat onder andere inhoudt dat er voldoende waarborgen worden getroffen tegen willekeur en misbruik door de bevoegde autoriteiten en dat burgers de effecten van een maatregel moeten kunnen inschatten.[11] Als praktische handvatten hanteert het EHRM drie leidende beginselen, te weten transparantie, effectieve notificatie en het zwaarder worden van het foreseeability-vereiste naarmate de inbreuk op artikel 8 lid 1 EVRM toeneemt.[12]

14. De overheid schiet op deze punten tekort:

- De Nederlandse burger wordt vaker aan het middel aftappen onderworpen dan waar dan ook in de (Westerse) wereld. Paul Frielink, Advocaat-Generaal en hoogleraar Openbaar Ministerie aan de Universiteit Maastricht, stelt in dagblad Trouw zelfs dat er in Nederland teveel telefoontaps worden geplaatst.[13]
- De weging door de rechter-commissaris zou volgens de Minister garanderen dat er sprake is van een proportionele inzet van het middel, maar dit dit rijmt niet met deze Nederlandse praktijk. Wij weten namelijk niet, hoe vaak een rechter-commissaris een verzoek tot aftappen *weigert*.
- Het Openbaar Ministerie blijkt geregeld gesprekken met geheimhouders te bewaren en soms worden deze ten onrechte opgenomen in het strafdossier. Als het gaat om schendingen van het beroepsgeheim door inlichtigendiensten tast de balie volledig in het duister. Hieruit blijkt een onzorgvuldigheid en achteloosheid aan de zijde van de Nederlandse overheid.
- De Minister wil ook de effectiviteit van aftappen in niet meer dan algemene termen toelichten. De Minister verwijst naar een onderzoek uit 2004, terwijl het meest recente onderzoek uit 2005 juist concludeerde dat de effectiviteit van aftappen afneemt.[14]
- Dit steekt des te meer nu in andere landen veel meer transparantie wordt geboden over aftappen. In de Verenigde Staten wordt ieder jaar een 'Wiretap Report” gepubliceerd, dat gedetailleerde cijfers bekendmaakt over de hoeveelheid taps en het aantal veroordelingen dat hierop volgde (zie **bijlage 1** voor het rapport uit 2008).[15] In het Verenigd Koninkrijk wordt ieder jaar een 30-pagina's tellend rapport hierover uitgegeven (zie **bijlage 2** voor het rapport uit 2008).[16]

---

10 Vgl. “procedures to be followed for examining, using and storing intercepted material, inter alia, should be set out in a form which is open to public scrutiny and knowledge”, zie EHRM in de zaak Liberty, par. 67.

11 Zie een uitgebreide samenvatting in EHRM Liberty, par. 62.

12 Zie EHRM Silver, par. 88 en EHRM Vogt, par. 48.

13 Zie http://www.trouw.nl/nieuws/nederland/article2867598.ece/_Justitie_tapt_te_veel_telefoons_.html.

14 Zie *Aftapbaarheid van Telecommunicatie*, TILT/Dialogic 2005, p.67-69.

15 Zie http://www.uscourts.gov/wiretap08/2008WTText.pdf.

16 Zie http://www.official-documents.gov.uk/document/hc0809/hc09/0901/0901.pdf.

15. Het is opmerkelijk dat de Minister slechts schrijft dat het Kabinet geen aanleiding ziet “een systeem [op te zetten] waarbij achteraf de effectiviteit van elke tap wordt gemeten”. Dat wordt niet nader toegelicht, terwijl het duidelijk moge zijn dat juist *dit* een heikel punt is in de beoordeling van de verenigbaarheid met artikel 8 EVRM. Waarom is de Minister niet bereid om een fundamentele discussie over het nut van aftappen aan te gaan?

16. Ook de notificatieplicht wordt al jaren massaal genegeerd en Bits of Freedom heeft nog onvoldoende verbetering kunnen zien:[17]

- Het WODC merkt in een rapport uit 2004 op dat in de praktijk dit voorschrift niet blijkt te worden nageleefd, omdat notificatie geen prioriteit heeft binnen het Openbaar Ministerie en er geen sanctie staat op het uitblijven ervan.[18]
- Uit een evaluatie uit 2007 is vervolgens op te maken dat het Openbaar Ministerie nog steeds niet volledig voldoet aan de notificatieplicht, maar dat de situatie “aanmerkelijk verbeterd” is.[19] In deze brief wordt onder meer aanbevolen een instructie op te stellen, een landelijke standaard procesbeschrijving te ontwikkelen en concrete afspraken te maken met falende parketten. Daarbij wordt gemeld dat het College van procureurs-generaal de uitvoering van deze aanbevelingen “nauwlettend” zal volgen.
- Op 11 november j.l. schrijft de Pers echter, dat het college van procureurs-generaal hierover nog steeds geen cijfers blijkt te hebben.[20] Ook over de instructie notificatieplicht is sindsdien niets meer vernomen.

17. Het uitblijven van notificatie versterkt de inbreuk op artikel 8 lid 1 EVRM, omdat de burger niet kan weten of en wanneer hij onderworpen is (geweest) aan afluisterpraktijken door de autoriteiten. Dit veroorzaakt een “chilling effect” bij de normale burger, een verhindering van het op legitieme wijze ongehinderd gebruikmaken van telecommunicatie door burgers, uit angst voor daaruit voortvloeiende strafprocesrechtelijke maatregelen, zoals afluisteren. Het Duitse Constitutionele Hof beziet het in de Duitse Grondwet verankerde telecommunicatiegeheim steeds vanuit het perspectief van deze “chilling effects”.[21]

18. Op de derde plaats wordt het voldoen aan bovenstaande deelcriteria van voorzienbaarheid (transparantie en notificatie) zwaarder, naarmate de inbreuk op artikel 8 lid 1 EVRM groter is. Nu de informatieverstrekking van de Minister ernstig tekortschiet op het gebied van de transparantie, en de notificatieplicht in Nederland onvoldoende wordt nageleefd, is ook aan dit derde beginsel onder de voorzienbaarheid van de aftapbevoegdheden niet voldaan.

**Het gebrek aan transparantie brengt risico's met zich voor de rechtstaat**

19. De onzorgvuldigheid en de geheimhouding waarmee de overheid het aftapbeleid omgeeft, druist ook in tegen een elementair beginsel van de rechtstaat. De brief en de beantwoording

17 Er is het recht van de burger op notificatie op grond van artikel 126bb Wetboek van Strafvordering, zodra het opsporingsonderzoek dat toestaat.

18 Zie“Evaluatie Wet bijzondere opsporingsbevoegdheden”, WODC, *Kamerstukken II* 29 441, nr.3, p.5

19 *Kamerstukken II* 29940, nr. 4, p.1-2.

20 Zie http://www.depers.nl/binnenland/352089/Afluisteren-het-kan-altijd-meer.html.

21 Bundesverfassungsgericht 11 maart 2008, 1 BvR 256/08, par. 122-123. In par. 123 oordeelt het BVerfG: “Die anlasslose Vorratsspeicherung von Telekommunikations-Verkehrsdaten könne die Bevölkerung massiv einschüchtern.” [einschüchtern = intimideren]).

van de Minister verhinderen controle op de uitoefening van de strafvordelijke bevoegdheid van aftappen en controle op het kabinetsbeleid.[22]

20. Bits of Freedom vraagt zich af waarom er geen serieuzere pogingen worden ondernomen om het parlement in te lichten over de toepassing van de aftapbevoegdheden. In antwoord op vraag 5 van het CDA – of er in Nederland voldoende waarborg en garantie is dat er geen wildgroei bestaat tegen het inzetten van de taps – wordt voor de zoveelste keer aan het Parlement de strafvorderlijke bevoegdheden aan het Parlement voorgelezen, maar van daadwerkelijke informatieverstrekking is geen sprake. De verantwoordelijkheid voor de "checks and balances" in onze rechtstaat liggen niet alleen bij de rechter-commissaris, maar dienen ook aan het parlement toe te komen.

**Het gebrek aan transparantie kan een negatieve uitwerking op de veiligheid hebben**

21. De twee hoofdargumenten om de informatieverstrekking te beperken (het niet beschikbaar zijn van de informatie en staatsgeheim) doen tenslotte afbreuk aan het beschermen van de veiligheid van burgers. Door het gebrek aan transparantie over de toepassing van de aftapbevoegdheden worden wetenschap en *civil society* niet in staat gesteld om de toepassing van de aftapbevoegdheden met waardevolle inzichten te voeden.[23] Zo dateert het laatste omvangrijke onderzoek over het opsporingsmiddel aftappen alweer uit 2005, terwijl – zoals wij al zagen – een van de hoofdconclusies uit dat onderzoek was dat het middel als zodanig in de komende jaren aan effectiviteit zou inleveren.

22. Vier jaar na dit onderzoek blijft zowel het parlement als de samenleving achter met enerzijds de constatering dat de afluisterbevoegdheden steeds vaker worden ingezet, terwijl de effectiviteit afneemt en het kabinet met schijnbare achteloosheid omspringt met de toepassing van de bevoegdheden. Hiermee wordt afbreuk gedaan aan de legitimiteit van de opsporing. Het risico bestaat dat de opsporingsdiensten minder serieus genomen worden door potentiële criminelen, en dat de samenleving hierdoor minder veilig wordt.

**Noodzaak, transparantie en notificatie moeten terug in het Nederlandse aftapbeleid**

23. Bits of Freedom roept op tot een fundamentele herbezinning van de afluisterpraktijken in Nederland. De toepassing van de aftapbevoegheid in Nederland is onwaardig aan een democratische rechtstaat. De Nederlandse burger wordt bijzonder vaak blootgesteld aan ernstige inbreuken op de persoonlijke levenssfeer en wordt daarvan niet of nauwelijks op de hoogte gesteld, terwijl de effectiviteit van zoveel taps onvoldoende duidelijk is en er nauwelijks sprake is van verantwoording door het Kabinet of controle door het parlement. Noodzaak, transparantie en notificatie moeten daarom terug in het Nederlandse aftapbeleid:

    - In concrete zin beveelt Bits of Freedom allereerst aan **om een strenger toetsingskader te ontwikkelen**. Het criterium "noodzakelijk in een democratische samenleving" moet voorafgaand aan iedere tap ook door de Officier van Justitie worden getoetst. Bovendien moet de rechter-commissaris zijn beslissing om wel of niet een tapbevel te geven (schriftelijk) motiveren aan de hand van dit toetsingskader. In dit

22 Zie EHRM in de zaak Liberty, par. 69.

23 Zoals betoogd door "D.J. Solove, Data mining and the security-liberty debate, University of Chicago Law review 2008, p.361".

toetsingskader dient de effectiviteit een belangrijke plaats in te nemen, alsmede de subsidiariteit, oftewel de vraag of het onderzoek ook op minder inbreukmakende wijze tot een goed einde kan worden gebracht. Bij deze laatste vraag dient de inbreuk die het plaatsen van een tap op de persoonlijke levenssfeer van derden eveneens te worden meegewogen.

- Op de tweede plaats roept Bits of Freedom het kabinet op om het **aftapbeleid op een veel transparantere** wijze te verantwoorden. De brief en de beantwoording van Minister over de aftapstatistieken moeten voortaan meer informatie bevatten over de toepassing van de aftapbevoegdheden. Het aantal afwijzingen van aftapverzoeken door de rechter-commissaris moet worden genoemd en het aantal aftapverzoeken moet opgesplitst worden per opsporingsdienst, per regio en per grondslag in het Wetboek van Strafrecht (i.e. per delict). Ook moet het aantal internettaps worden gepubliceerd. Tevens dient inzicht te worden gegeven in de mate waarin iedere individuele tap heeft bijgedragen aan het opsporingsonderzoek.
- **Op de derde plaats dient de notificatieplicht eindelijk serieus genomen te worden**, zodat burgers die onderworpen zijn geweest aan dit opsporingsmiddel, in staat worden gesteld het rechtmatig gebruik van de bevoegdheden te controleren.

**Over Bits of Freedom**

Bits of Freedom verdedigt burgerrechten in de digitale wereld, waaronder het recht op privacy. Zij doet dat door constructieve campagnes te voeren en de overheid te informeren. Het belang van de burger staat daarbij centraal.

Bits of Freedom vertrouwt erop u hiermee voldoende te hebben geïnformeerd en houdt zich graag beschikbaar voor een nadere toelichting als daaraan behoefte bestaat.

Hoogachtend,

Axel Arnbak

**BIJLAGE 1**

# Contents



# Text Tables

# Appendix Tables

# Report of the Director of the Administrative Office of the United States Courts

## on

## Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications

The Omnibus Crime Control and Safe Streets Act of 1968 requires the Administrative Office of the United States Courts (AO) to report to Congress the number and nature of federal and state applications for orders authorizing or approving the interception of wire, oral, or electronic communications. The statute requires that specific information be provided to the AO, including the offense(s) under investigation, the location of the intercept, the cost of the surveillance, and the number of arrests, trials, and convictions that directly result from the surveillance. This report covers intercepts concluded between January 1, 2008, and December 31, 2008, and provides supplementary information on arrests and convictions resulting from intercepts concluded in prior years.

A total of 1,891 intercepts authorized by federal and state courts were completed in 2008, a decrease of 14 percent compared to the number terminated in 2007. The number of applications for orders by federal authorities fell 16 percent to 386. The number of applications reported by state prosecuting officials dropped 14 percent to 1,505, with 22 states providing reports, two fewer than in 2007. Installed wiretaps were in operation an average of 41 days per wiretap in 2008, compared to 44 days in 2007. The average number of persons whose communications were intercepted decreased from 94 per wiretap order in 2007 to 92 per wiretap order in 2008. The average percentage of intercepted communications that were incriminating was 19 percent in 2008, compared to 30 percent in 2007.

Public Law 106-197 amended 18 U.S.C. 2519(2)(b) to require that reporting should reflect the number of wiretap applications granted for which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2008, two instances were reported of encryptions encountered during state wiretaps; neither prevented officials from obtaining the plain text of the communications.

The appendix tables of this report list all intercepts reported by judges and prosecuting officials for 2008. Appendix Table A-1 shows reports filed by federal judges and federal prosecuting officials. Appendix Table B-1 presents the same information for state judges and state prosecuting officials. Appendix Tables A-2 and B-2 contain information from the supplementary reports submitted by prosecuting officials about additional arrests and trials in 2008 arising from intercepts initially reported in prior years.

Title 18 U.S.C. Section 2519(2) provides that prosecutors must submit wiretap reports to the AO no later than January 31 of each year. This office, as is customary, sends a letter to the appropriate officials every year reminding them of the statutory mandate. Nevertheless, each year reports are received after the deadline has passed, and the filing of some reports may be delayed to avoid jeopardizing ongoing investigations. A total of 54 state and local prosecutors' reports were missing in 2008, compared to 56 in 2007. Information received after the deadline will be included in next year's *Wiretap Report*. The AO is grateful for the cooperation and the prompt response we received from many officials around the nation.

James C. Duff
Director

April 2009

# Applications for Orders Authorizing or Approving the Interception of Wire, Oral, or Electronic Communications

## Reporting Requirements of the Statute

Each federal and state judge is required to file a written report with the Director of the Administrative Office of the United States Courts (AO) on each application for an order authorizing the interception of a wire, oral, or electronic communication (18 U.S.C. 2519(1)). This report is to be furnished within 30 days of the denial of the application or the expiration of the court order (after all extensions have expired). The report must include the name of the official who applied for the order, the offense under investigation, the type of interception device, the general location of the device, and the duration of the authorized intercept.

Prosecuting officials who applied for interception orders are required to submit reports to the AO each January on all orders that were terminated during the previous calendar year. These reports contain information related to the cost of each intercept, the number of days the intercept device was actually in operation, the total number of intercepts, and the number of incriminating intercepts recorded. Results such as arrests, trials, convictions, and the number of motions to suppress evidence related directly to the use of intercepts also are noted.

Neither the judges' reports nor the prosecuting officials' reports contain the names, addresses, or phone numbers of the parties investigated. The AO is **not** authorized to collect this information.

This report tabulates the number of applications for interceptions that were granted or denied, as reported by judges, as well as the number of authorizations for which interception devices were installed, as reported by prosecuting officials. No statistics are available on the number of devices installed for each authorized order. This report does not include interceptions regulated by the Foreign Intelligence Surveillance Act of 1978 (FISA).

No report to the AO is required when an order is issued with the consent of one of the principal parties to the communication. Examples of such situations include the use of a wire interception to investigate obscene phone calls, the interception of a communication to which a police officer or police informant is a party, or the use of a body microphone. Also, no report to the AO is required for the use of a pen register (a device attached to a telephone line that records or decodes impulses identifying the numbers dialed from that line) unless the pen register is used in conjunction with any wiretap devices whose use must be reported. Pursuant to 18 U.S.C. 3126, the U.S. Department of Justice collects and reports data on pen registers and trap and trace devices.

### Regulations

The Director of the AO is empowered to develop and revise the reporting regulations and reporting forms for collecting information on intercepts. Copies of the regulations, the reporting forms, and the federal wiretapping statute may be obtained by writing to the Administrative Office of the United States Courts, Statistics Division, Washington, D.C. 20544.

The Attorney General of the United States, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any specially designated Deputy Assistant Attorney General in the Criminal Division of the Department of Justice may authorize an application to a federal judge for an order authorizing the interception of wire, oral, or electronic communications. On the state level, applications are made by a prosecuting attorney "if such attorney is authorized by a statute of that State to make application to a State court judge of competent jurisdiction."

Many wiretap orders are related to large-scale criminal investigations that cross county and state boundaries. Consequently, arrests, trials, and convictions resulting from these interceptions often do not occur within the same year as the installation of the intercept device. Under 18 U.S.C. 2519(2), prosecuting officials must file supplementary reports on additional court or police activity that occurs as a result of intercepts reported in prior years. Appendix Tables A-2 and B-2 describe the additional activity reported by prosecuting officials in their supplementary reports.

Table 1 shows that 47 jurisdictions (the federal government, the District of Columbia, the Virgin Islands, and 44 states) currently have laws that authorize courts to issue orders permitting wire, oral, or electronic surveillance. During 2008, a total of 23 jurisdictions reported using at least one of these three types of surveillance as an investigative tool.

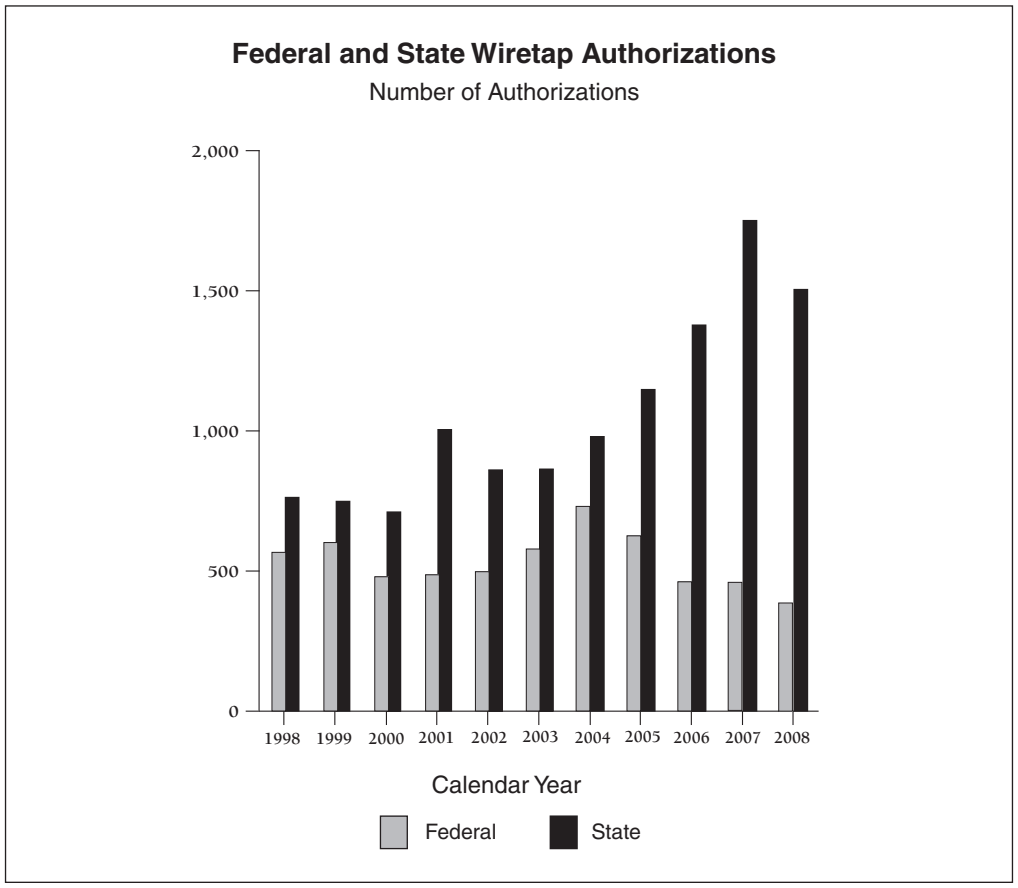
## Summary and Analysis of Reports by Judges

Data on applications for wiretaps terminated during calendar year 2008 appear in Appendix Tables A-1 (federal) and B-1 (state). The reporting numbers used in the appendix tables are reference numbers assigned by the AO; these numbers do not correspond to the authorization or application numbers used by the reporting jurisdictions. The same reporting number is used for any supplemental information reported for a communications intercept in future volumes of the *Wiretap Report*.

The number of wiretaps reported decreased 14 percent in 2008. A total of 1,891 applications were reported as authorized in 2008, including 386 submitted to federal judges and 1,505 to state judges. No applications were denied. Compared to the number approved during 2007, the number of applications reported as approved by federal judges in 2008 fell 16 percent. The number of applications approved by state judges declined 14 percent. Wiretap applications in New York (433 applications), California (418 applications), New Jersey (175 applications), and Florida (102 applications) accounted for 75 percent of all applications approved by state judges. The number of states reporting wiretap activity was lower than the number for last year (22 states reported such activity in 2008, compared to 24 in 2007). In 2008, a total of 110 separate state jurisdictions (including counties, cities, and judicial districts) submitted reports, which is 7 fewer than the total for 2007.

### Authorized Lengths of Intercepts

Table 2 presents the number of intercept orders issued in each jurisdiction that provided reports, the number of amended intercept orders issued, the number of extensions granted, the average lengths of



the original authorizations and their extensions, the total number of days the intercepts actually were in operation, and the nature of the location where each interception of communications occurred. Most state laws limit the period of surveillance under an original order to 30 days. This period, however, can be lengthened by one or more extensions if the authorizing judge determines that additional time for surveillance is warranted.

During 2008, the average length of an original authorization was 29 days, the same average length as in 2007. A total of 1,266 extensions were requested and authorized in 2008, a decrease of 26 percent. The average length of an extension remained unchanged at 29 days. The longest federal intercepts occurred in two districts, the Central District of California and the Southern District of Texas, where the original 30-day orders were extended 6 times in each district to complete 2 wiretaps lasting 210 days that were used in racketeering and narcotics investigations, respectively. Among state wiretaps terminating during 2008, the longest was used in a narcotics investigation conducted by the New York Organized Crime Task Force; this wiretap, in use for 590 days, required the original order to be extended 20 times. In contrast, 12 federal intercepts and 70 state intercepts were in operation for less than a week.

## Locations

The most common location specified in wiretap applications authorized in 2008 was "portable device, carried by/on individual," a category included for the first time in the *2000 Wiretap Report*. This category was added because wiretaps authorized for devices such as portable digital pagers and cellular telephones did not fit readily into the location categories provided prior to 2000. Since that time, the proportion of wiretaps involving fixed locations has declined as the use of mobile communications devices has become more prevalent. Table 2 shows that in 2008, a total of 95 percent (1,793 wiretaps) of all intercepts authorized involved portable devices such as these, which are not limited to fixed locations. This is a slight increase from 2007, when 94 percent of all intercepts involved portable devices.

The next most common location reported for the placement of wiretaps in 2008 was a combination of locations, which was noted in 38 applications (2 percent of the total). The category "personal residence," a type of location that includes single-family houses as well as row houses, apartments, and other multi-family dwellings, was the third most common location cited. Table 2 shows that in 2008, almost 2 percent of all intercept devices (31 wiretaps) were authorized for personal residences. Ten wiretaps were authorized for "other" locations, which included such places as prisons, pay telephones in public areas, and motor vehicles. Six wiretaps were authorized for business establishments such as offices, restaurants, and hotels. Together, "other" and business establishments accounted for less than 1 percent of all intercepts authorized.

Pursuant to the Electronic Communications Privacy Act of 1986, a specific location need not be cited if the application contains a statement explaining why such specification is not practical or shows "a purpose, on the part of that person (under investigation), to thwart interception by changing facilities" (see 18 U.S.C. 2518 (11)). In these cases, prosecutors use "roving" wiretaps to target a specific person rather than a specific telephone or location. The Intelligence Authorization Act of 1999, enacted on October 20, 1998, amended 18 U.S.C. 2518 (11)(b) to provide that a specific facility need not be cited "if there is probable cause to believe that actions by the person under investigation could have the effect of thwarting interception from a specified facility." The amendment also specifies that "the order authorizing or approving the interception is limited to interception only for such time as it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communication will be or was transmitted."

For 2008, authorizations for 11 wiretaps indicated approval with a relaxed specification order, meaning they were considered roving wiretaps. This is a decrease from 2007, when 21 wiretaps were reported as roving wiretaps. All 11 roving wiretaps were reported by state authorities: 6 were used in racketeering investigations, and 5 in a narcotics investigations.

## Offenses

Violations of drug laws and homicide/assault were the two most prevalent types of offenses investi-

gated through communications intercepts. Racketeering was the third most frequently recorded offense category, and gambling the fourth. Table 3 indicates that 84 percent of all applications for intercepts (1,593 wiretaps) authorized in 2008 cited a drug offense as the most serious offense under investigation. Many applications for court orders indicated that several criminal offenses were under investigation, but Table 3 includes only the most serious criminal offense named in an application. The use of federal intercepts to conduct drug investigations was most common in the Central District of California (33 applications), the Southern District of New York (30 applications), and the Southern District of Texas (21 applications). On the state level, the largest numbers of drug-related intercepts were reported by Los Angeles County of California (164 applications), Queens County of New York (118 applications), and the New York City Special Narcotics Bureau (101 applications). Nationwide, homicide/assault was specified in 5 percent of applications (92 orders) as the most serious offense under investigation. Racketeering was specified in 3 percent of applications (58 orders) as the most serious offense under investigation. The category of gambling was specified in almost 3 percent of applications (54 orders). One other offense category in Table 3 with a significant total was larceny (43 orders).

## Summary and Analysis of Reports by Prosecuting Officials

In accordance with 18 U.S.C. 2519(2), prosecuting officials must submit reports to the AO no later than January 31 of each year for intercepts terminated during the previous calendar year. Appendix Tables A-1 and B-1 contain information from all prosecutors' reports submitted for 2008. Judges submitted 54 reports for which the AO received no corresponding reports from prosecuting officials. For these authorizations, the entry "NP" (no prosecutor's report) appears in the appendix tables. Some of the prosecutors' reports may have been received too late to include in this report, and some prosecutors delayed filing reports to avoid jeopardizing ongoing investigations. Information received after the deadline will be included in next year's *Wiretap Report*.

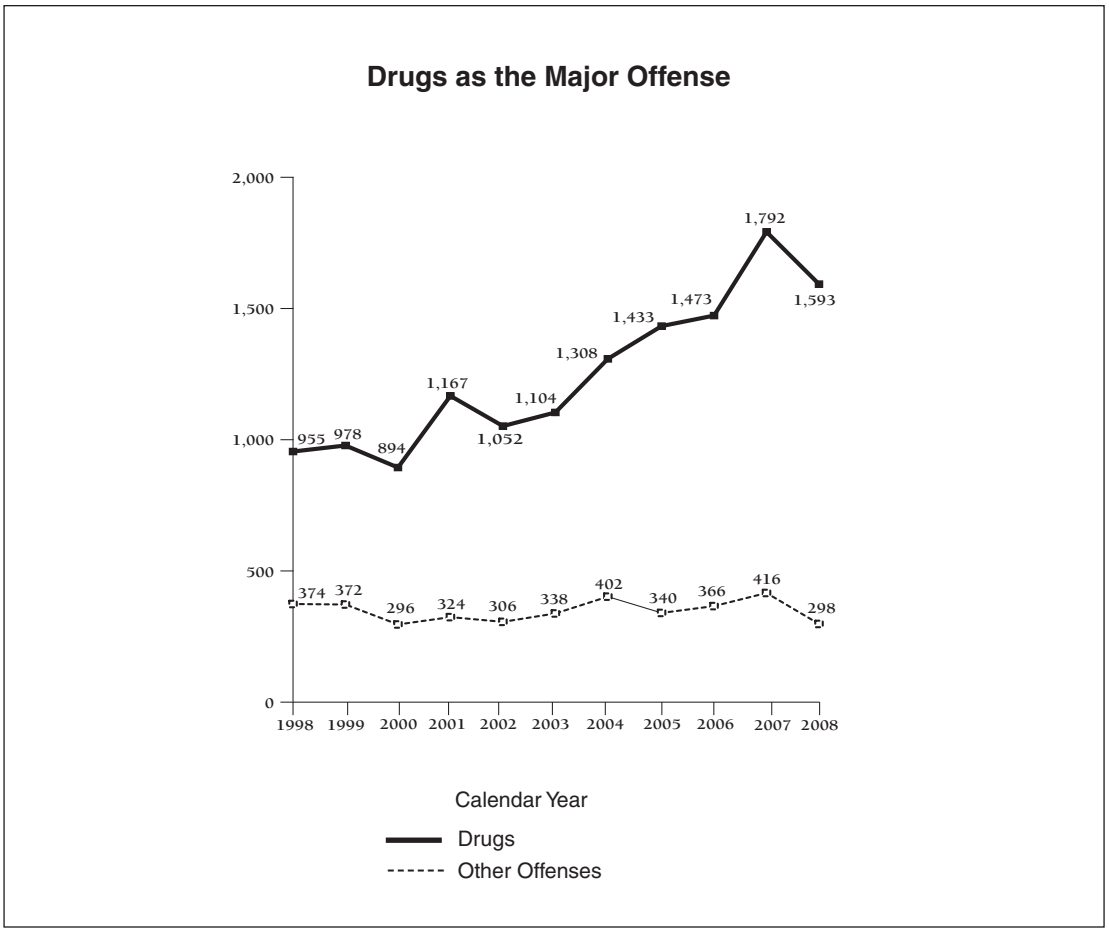
### Nature of Intercepts

Of the 1,891 communication interceptions authorized in 2008, reports submitted by prosecutors indicated that intercept devices were installed and results were reported in conjunction with a total of 1,809 orders. As shown in Table 2, orders for 28 wiretaps were approved for which no wiretaps actually were installed, and results from 54 wiretap orders were not available for reporting by the prosecutors. Table 4 presents information on the average number of intercepts per order, the number of persons whose communications were intercepted, the total number of communications intercepted, and the number of incriminating intercepts. Wiretaps varied extensively with respect to the above characteristics.

In 2008, installed wiretaps were in operation an average of 41 days, 3 days fewer than the average number of days wiretaps were in operation in 2007. Three interrelated federal wiretaps with the most intercepts occurred in the Northern District of Illinois, where narcotics investigations involving cellular telephones and other electronic communications resulted in the interception of 104,777 messages. The federal wiretap with the second highest number of intercepts, a cellular telephone wiretap, occurred in the Southern District of California as part of a narcotics investigation; this wiretap was active for 60 days and resulted in a total of 33,419 interceptions.

The state wiretap with the most intercepts was conducted by the New York Organized Crime Task Force, which used a 590-day wiretap in a narcotics investigation involving cellular telephones and oral communications that resulted in the interception of 168,292 messages, 18,353 of which were incriminating. A second wiretap installed by the New York Organized Crime Task Force lasted 219 days and generated a total of 58,926 cellular and standard telephone intercepts.

Nationwide, in 2008 the average number of persons whose communications were intercepted per order in which intercepts were installed was 92, and the average number of communications intercepted was 2,707 per wiretap. An average of 514 intercepts per installed wiretap produced incriminating evidence. The average percentage of incriminating intercepts per order decreased from 30 percent in 2007 to 19 percent in 2008.




The three major categories of surveillance are wire communications, oral communications, and electronic communications. In the early years of wiretap reporting, nearly all intercepts involved telephone (wire) surveillance, primarily communications made via conventional telephone lines; the remainder involved microphone (oral) surveillance or a combination of wire and oral interception. With the passage of the Electronic Communications Privacy Act of 1986, a third category was added for the reporting of electronic communications, which most commonly involve digital-display paging devices or fax machines, but also may include some computer transmissions.

Table 6 presents the type of surveillance method used for each intercept installed. The most common method of surveillance reported was "phone wire communication," which includes all telephones (land line, cellular, cordless, and mobile). Telephone wiretaps accounted for 97 percent (1,757 cases) of intercepts installed in 2008.

The next most common method reported was a combination of surveillance devices, which usually includes a mobile/cellular telephone with another type of oral or electronic device. Combined wiretaps were used in 2 percent of intercepts (33 cases). In 2008, a combination intercept reported for Middlesex County in Massachusetts included cellular and standard telephones, a microphone, and a fax machine. The electronic wiretap, which includes digital display pagers, voice pagers, fax machines, and transmissions via computer such as electronic mail, accounted for less than 1 percent (10 cases) of intercepts installed in 2008.

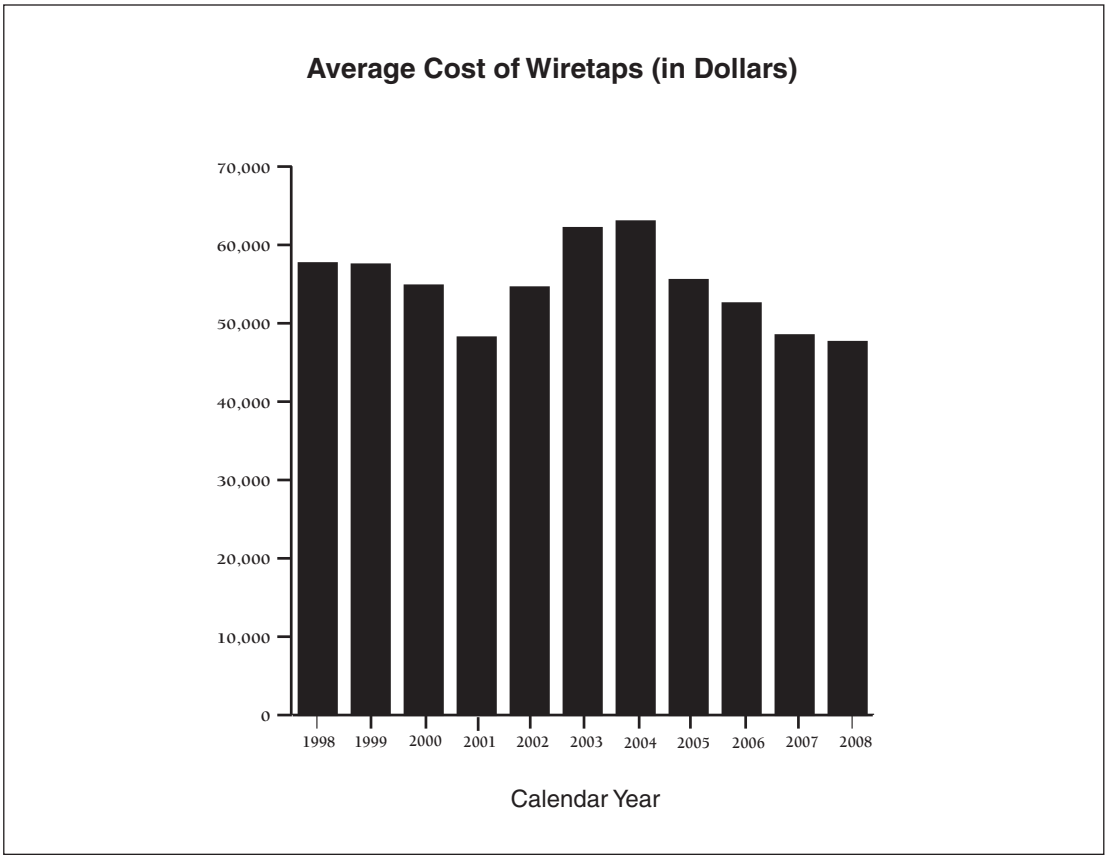
Public Law 106-197 amended 18 U.S.C. 2519(2)(b) in 2001 to require that reporting should reflect the number of wiretap applications granted in which encryption was encountered and whether such encryption prevented law enforcement officials from obtaining the plain text of communications intercepted pursuant to the court orders. In 2008, encryption was encountered during two state wiretaps; neither instance prevented officials from obtaining the plain text of the communications.

## Costs of Intercepts

Table 5 provides a summary of expenses related to intercept orders in 2008. The expenditures noted reflect the cost of installing intercept devices and monitoring communications for the 1,703 authorizations for which reports included cost data. The average cost of intercept devices installed in 2008 was $47,624, down 2 percent from the average cost in 2007. For federal wiretaps for which expenses were reported in 2008, the average cost was $70,536, a 7 percent increase from the average cost in 2007. The average cost of a state wiretap declined 6 percent to $41,154 in 2008. For additional information, see Appendix Tables A-1 (federal) & B-1 (state).

## Arrests and Convictions

Table 6 presents the numbers of persons arrested and convicted as a result of interceptions reported as terminated in 2008. As of December 31, 2008, a total of 4,133 persons had been arrested based on interceptions of wire, oral, or electronic communications, 14 percent fewer than in 2007. Wiretaps terminated in 2008 resulted in the conviction of 810 persons as of December 31, 2008, which was 20 percent of the number of persons arrested. Federal wiretaps were responsible for 38 percent of the arrests and 29 percent of the convictions arising from wiretaps during 2008. The Central District of California reported the most arrests arising from a federal wiretap terminated in 2008; seven related wiretaps in a racketeering investigation there yielded the arrest of 118 persons. A wiretap in Maricopa County, Arizona, which caused the most arrests of any state intercept terminated in 2008, led to arrest of 65 persons in connection with a narcotics investigation. The leader among state intercepts in producing convictions was a wiretap authorized in the 11th Judicial District (Hamilton), Tennessee, for a narcotics investigation, which resulted in the conviction of 40 of the 43 persons arrested. The next-largest number of convictions reported to have stemmed from a state wiretap occurred in Queens County, New York, where the lead wiretap of 50 intercept orders authorized in a theft investigation yielded the conviction of 33 persons. The Southern District of Ohio reported the most convictions for any federal wiretap; there the lead wiretap of 2 intercepts authorized in a narcotics investigation produced convictions for 30 of the 31 persons arrested.



Federal and state prosecutors often note the importance of electronic surveillance in obtaining arrests and convictions. Speaking of a 60-day surveillance of cellular telephone communications during a federal narcotics investigation in the Northern District of Texas, the reporting official stated that this wiretap allowed identification of illegal activities that resulted in the arrest of 17 individuals and the seizure of 370 kilos of cocaine, 360 pounds of methamphetamine, 20 weapons, 5 vehicles, and $8 million in cash. In the Eastern District of Virginia, a routine federal narcotics surveillance identified incriminating cellular telephone communications that led to the arrest of 16 individuals and conviction of 10, as well as the seizure of $2.3 million, 7 weapons, and 2 vehicles.

At the state level, San Diego County reported that a multi-jurisdiction case involving a cellular telephone wiretap resulted in the seizure of 52 kilos of cocaine and $2 million, along with the arrest of 47 individuals and the conviction of 25. The New York City Special Narcotics Bureau reported that a cellular telephone wiretap led to the seizure of 180 kilos of cocaine and $400,000. In a separate narcotics investigation, the New York City Special Narcotics Bureau reported that interceptions obtained from a cellular telephone wiretap conducted over 36 days in a narcotics investigation resulted in the seizure of approximately 30 kilos of cocaine and $22,000.

Because criminal cases involving the use of surveillance may still be under active investigation or prosecution, the final results of many of the wiretaps concluded in 2008 may not have been reported. Prosecutors will report additional costs, arrests, trials, motions to suppress evidence, and convictions related directly to these intercepts in future supplementary reports, which will be noted in Appendix Tables A-2 and B-2 of subsequent volumes of the Wiretap Report.

## Summary of Reports for Years Ending December 31, 1998 Through 2008

Table 7 provides information on intercepts reported each year from 1998 to 2008. This table specifies the number of intercept applications requested, authorized, and installed; the number of extensions granted; the average length of original orders and extensions; the locations of intercepts; the major offenses investigated; average costs; and the average number of persons intercepted, communications intercepted, and incriminating intercepts. From 1998 to 2008, the number of intercept applications authorized by year (as reported through 2008) increased 42 percent. The majority of wiretaps consistently have been used for drug crime investigations, which accounted for 84 percent of intercept applications in 2008. Between 1998 and 2008, the percentage of drug-related wiretaps ranged from 72 percent to 84 percent of all authorized applications.

## Supplementary Reports

Under 18 U.S.C. 2519(2), prosecuting officials must file supplementary reports on additional court or police activity occurring as a result of intercepts reported in prior years. Because many wiretap orders are related to large-scale criminal investigations that cross county and state boundaries, supplementary reports are necessary to fulfill reporting requirements. Arrests, trials, and convictions resulting from these interceptions often do not occur within the same year in which the intercept was first reported. Appendix Tables A-2 and B-2 provide detailed data from all supplementary reports submitted.

During 2008, a total of 3,311 arrests, 2,698 convictions, and additional costs of $31,076,214 arose from and were reported for wiretaps completed in previous years. Table 8 summarizes additional prosecution activity by jurisdiction from supplemental reports on intercepts terminated in the years noted. Sixty-six percent of the supplemental reports of additional activity in 2008 involved wiretaps terminated in 2007. Of all supplemental arrests, convictions, and costs reported in 2008, intercepts concluded in 2007 led to 52 percent of arrests, 44 percent of convictions, and 72 percent of expenditures. Table 9 reflects the total number of arrests and convictions resulting from intercepts terminated in calendar years 1998 through 2008. ■

**BIJLAGE 2**

# Report of the Interception of Communications Commissioner for 2008

Commissioner:
THE RT HON SIR PAUL KENNEDY

Presented to Parliament by the Prime Minister
pursuant to section 58(6) of the
Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed
21 July 2009

Laid before the Scottish Parliament by
the Scottish Ministers
July 2009

HC 901
SG/2009/138

£5.50

# Report of the Interception of Communications Commissioner for 2008

Commissioner:
THE RT HON SIR PAUL KENNEDY

Presented to Parliament by the Prime Minister
pursuant to section 58(6) of the
Regulation of Investigatory Powers Act 2000

Ordered by the House of Commons
to be printed
21 July 2009

Laid before the Scottish Parliament by
the Scottish Ministers
July 2009

HC 901
SG/2009/138

£5.50

ISBN: 978 0 10 296236 9

# Contents

From: The Right Honourable Sir Paul Kennedy

The Interception of Communications
Commissioner
c/o 2 Marsham Street
London SW1P 4DF

13 July 2009

I enclose my third Annual Report on the discharge of my functions under the Regulation of Investigatory Powers Act 2000. The Report covers the period 1 January 2008 to 31 December 2008. It is, of course, for you to decide, after consultation with me, how much of the report should be excluded from publication on the grounds that it is prejudicial to national security, to the prevention or detection of serious crime, to the economic well-being of the United Kingdom, or to the continued discharge of the functions of any public authority whose activities include activities subject to my review (section 58(7)) of the Act). Following the practice of my predecessors, I have taken the course of writing the report in two parts, the Confidential Annex containing those matters which in my view should not be published. I hope that this is a convenient course.

**Sir Paul Kennedy**

The Rt. Hon. Gordon Brown MP
10 Downing Street
London SW1A 2AA

# Annual Report of the Interception of Communications Commissioner for 2008

## Section 1: General

### Introduction

1.1 On 11 April 2006 I was appointed the Interception of Communications Commissioner under Section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA). My appointment is for a period of three years.

1.2. I am required by section 58(4) of RIPA as soon as practicable after the end of each calendar year to report with respect to the carrying out of my functions as the Interception of Communications Commissioner. This is my third annual report as Commissioner and it covers the period 1 January 2008 until 31 December 2008. In producing my report, I propose to follow, as my predecessors have done, the practice of writing the report in two parts, this main part for publication, the other part being a Confidential Annex to include those matters which cannot be fully explained without disclosing sensitive information.

### Functions of the Commissioner

1.3 I was appointed under section 57 of the Regulation of Investigatory Powers Act 2000 (RIPA). The coming into force of RIPA on 2 October 2000 coincided with the coming into force of the Human Rights Act 1998 (HRA) which incorporated the European Convention on Human Rights into UK law. These two important pieces of legislation brought about a number of changes in the law and in the practice of those responsible for the lawful interception of communications.

1.4 As Commissioner I have four main functions: these are set out in section 57 of RIPA and, for ease of reference, are as follows:

- To keep under review the carrying out by the Secretary of State of the functions conferred on him by sections 1 to 11 of RIPA and the adequacy of any arrangements made for the purpose of sections 15 and 16 of RIPA.
- To keep under review the exercise and performance by the Secretary of State of the powers and duties conferred or imposed by or under Chapter II of Part I (the acquisition and disclosure of communications data).
- To keep under review the exercise and performance by the Secretary of State in relation to information obtained under Part I of the powers and duties conferred or imposed on him by or under Part III (investigation of electronic data protected by encryption etc).
- To give the Investigatory Powers Tribunal set up under section 65 of RIPA all such assistance as the Tribunal may require for the purpose of enabling them to carry out their functions under that section.

### Discharge of my functions

1.5 Section 57(2) of RIPA provides that as the Interception of Communications Commissioner I shall keep under review:

(a) the exercise and performance by the Secretary of State of the power and duties conferred or imposed on him by or under sections 1 to 11;

(b) the exercise and performance, by the persons on whom they are conferred or imposed, of the powers and duties conferred or imposed by or under Chapter II of Part I;

(c) the exercise and performance by the Secretary of State in relation to information obtained under Part I of the powers and duties conferred or imposed on him by or under Part III; and

(d) the adequacy of the arrangements by virtue of which:

(i) the duty which is imposed on the Secretary of State by section 15; and

(ii) so far as is applicable to information obtained under Part I, the duties imposed by section 55

are sought to be discharged.

1.6 Part III (sections 49 to 56, together with Schedule 2) of RIPA – investigation of electronic data protected by encryption etc – contains provisions designed to maintain the effectiveness of existing law enforcement powers in the face of increasing criminal and hostile intelligence use of encryption (the means of scrambling electronic information into a secret code of letters, numbers and signals). Encrypted information cannot be unscrambled without a decoding key. Part III introduces a power to require disclosure of protected (encrypted) data. Parliament has now approved the Code of Practice for the investigation of protected electronic information; it came into force on 1 October 2007 and provides guidance for the authorities to follow when they require disclosure of protected electronic information.

# Section 2: Part I Chapter I – Interception of Communications

## General

*Oversight arrangements*

2.1 I have decided to continue with the practice followed by my predecessors of making twice yearly visits to the Security Service, the Secret Intelligence Service, Government Communications Headquarters, the Serious Organised Crime Agency, the Metropolitan Police Counter Terrorism Command, Strathclyde Police, the Police Service of Northern Ireland, the Northern Ireland Office, HM Revenue and Customs, the Foreign and Commonwealth Office, the Home Office, the Scottish Government and the Ministry of Defence. In short, I meet officers in the agencies undertaking interception work and officials in the departments of the Secretaries of State/Ministers which issue the warrants. Prior to each visit, I obtain a complete list of warrants issued or renewed or cancelled since my previous visit. I then select, largely at random, a sample of warrants for inspection. These include both warrants and attendant certificates. In the course of my visit I satisfy myself that those warrants fully meet the criteria of RIPA, that proper procedures have been followed and that the relevant safeguards and Codes of Practice have been followed. During each visit I review each of the files and the supporting documents and discuss the cases with the officers concerned. I can, if I need to, view the product of interception. It is of paramount importance to ensure that the facts justified the use of interception in each case and that those concerned with interception fully understand the safeguards and the Codes of Practice.

2.2 I continue to be impressed by the quality, dedication and enthusiasm of the personnel carrying out this work. They possess a detailed understanding of the legislation and are always anxious to ensure that they comply both with the legislation and the appropriate safeguards. All applications made to the Secretary of State are scrutinised by officials in the warrants unit within their respective

Department (e.g., the Home Office, the Foreign Office and the Ministry of Defence and by similar officers in departments in the Northern Ireland Office and Scottish Government). They are all skilled in their work and there is very little danger of any defective application being placed before the Secretary of State. I will refer in some detail to errors which have occurred during the period under review. Where errors have occurred, they are errors of detail or procedure and not of substance. If there is any product obtained through such errors it has been immediately destroyed. The Agencies always make available to me the personnel and documents that I have asked to see. They welcome my oversight, as ensuring that they are acting lawfully, proportionately and appropriately, and they seek my advice whenever it is deemed appropriate. It is a reassurance to the general public that their activities are overseen by an independent person who has held high judicial office. I am left in no doubt at all as to the Agencies' commitment to comply with the law. In case of doubt or difficulty, they do not hesitate to contact me and to seek advice.

*Meetings with the Secretaries of State*

2.3 During the period of this Report I met the Home Secretary, the Foreign Secretary, the Secretary of State for Defence and the Secretary of State for Northern Ireland. I was unable to meet the First Minister for Scotland but I did, however, meet the Cabinet Secretary for Justice who, in reality, signs most of the warrants in Scotland. It is clear to me that each of them gives a substantial amount of time and takes considerable care to satisfy himself or herself that the warrants are necessary for the authorised purposes, and that what is proposed is proportionate. If the Secretary of State wishes to have further information in order to be satisfied that he or she should grant the warrant then it is requested and given. Outright and final refusal of an application is comparatively rare, because the requesting agencies and the senior officials in the Secretary of State's Department scrutinise the applications with care before they are submitted for approval. However, the Secretary of State may refuse to grant the warrant if he or she considers, for example, that the strict requirements of necessity and proportionality are not met. The agencies are well aware that the Secretary of State does not act as a "rubber stamp".

*Visits to the communication service providers and internet service providers*

2.4 During 2008, I visited a total of nine communication service providers (CSPs) and internet service providers (ISPs) consisting of the Royal Mail and the communications companies who are most engaged in interception work. These visits, mostly outside London, are not formal inspections but are designed to enable me to meet both senior staff in each company as well as the personnel who carry out the work on the ground, and for them to meet and talk to me. I have no doubt that the staff in the CSPs and ISPs welcome these visits. We discussed the work that they do, the safeguards that are in place, any errors that have occurred, any legal or other issues which are of concern to them, and their relationships with the intercepting agencies. Those in the CSPs and ISPs who work in this field are committed and professional. They recognise the importance of the public interest, and the necessity of doing all their work accurately and efficiently, and show considerable dedication to it.

*Intelligence and Security Committee*

2.5 Along with the Intelligence Services Commissioner, Sir Peter Gibson, I attended the meeting of the Intelligence and Security Committee on 10 June 2008 for an informal discussion about our respective roles. There was a helpful exchange of views on a number of current issues including the work of the agencies over the last year and the challenges ahead, changes in number of warrants and authorisations, trends in the number of interception warrant breaches and errors, the admissibility of intercept as evidence and the Wilson Doctrine, about which I will say more at the end of this Report.

*Privy Council Review of Intercept as Evidence*

2.6 In paragraphs 2.6 – 2.7 of my Annual Report for 2007 I reported on the Prime Minister's announcement of a Privy Council Review of Intercept as Evidence under the chairmanship of Sir John Chilcot. In my Report I commented on the statement made by the Prime Minister to the House of Commons on 6 February 2008 accepting the committee's main conclusion that it should be possible to find a way to use some intercept material as evidence provided – and only provided – that certain key conditions can be met. The report sets out nine conditions in detail. They relate to complex and important issues, and include: giving the intercepting agencies the ability to retain control over whether their material is used in prosecutions; ensuring that disclosure of material cannot be required against the wishes of the agency originating the material; protecting the current close co-operation between intelligence and law enforcement agencies; and ensuring that agencies cannot be required to transcribe or make notes of material beyond a standard of detail that they deem necessary.

2.7 Since the Prime Minister's statement a lot of work has been done, led by the Home Office to see whether and how these issues and other conditions – intended to protect sensitive techniques, safeguard resources, and ensure that intercept can still be used effectively for intelligence – can be met. During 2008 I attended a number of meetings at the Home Office where I was fully briefed on the development of models under which material might be made available for use in criminal cases in England and Wales, strictly subject to all the Chilcot conditions being met. I know that operational live testing of these models took place in March and April 2009 followed by court role plays during May 2009. These highlighted real legal and operational difficulties inherent in using intercept as evidence within the UK; I cannot see a way to safely overcome these. Should the conclusion be that the Chilcot conditions cannot be fully met, I would welcome the government's acceptance that intercept as evidence should not be introduced. I look forward to being advised of the outcome of the court tests and to be able to comment on these in my 2009 Annual Report.

*The International Intelligence Review Agencies Conference*

2.8 Along with the Intelligence Services Commissioner, the Right Honourable Sir Peter Gibson, I attended the sixth international biennial conference of the International Intelligence Review Agencies in Auckland, New Zealand between 6 – 8 October 2008. The aim of the Conference was for the delegates to explore and exchange views on various principles or practices which were reasonably common between them, ranging from whose interests do the oversight mechanisms serve, to whether technology used by the agencies makes oversight reviews more difficult. I was asked, and gladly agreed, to address the conference on the *"Intrusion into individual privacy in search of intelligence – oversight role"*. Members of the Intelligence and Security Committee were also present. There were delegates from a number of countries from around the world – including Australia, Belgium, Canada, New Zealand, Poland, Republic of South Africa and the United States of America. I found the discussions during the conference and in the course of informal fringe discussions to be interesting, informative and valuable.

*House of Lords Select Committee on the Constitution*

2.9 On 21 May 2008 I gave oral evidence to the House of Lords Select Committee on the Constitution as part of their inquiry which sought answers to questions as to the impact that government surveillance and data collection have upon the privacy of citizens and their relationship with the State. I gladly offered my views drawn from my oversight experience as the Interception of Communications Commissioner. The Select Committee's two-volume Report "Surveillance: Citizens and the State" – Volume I: Report (HL Paper 18-I) and Volume II: Evidence (HL Paper 18-II) was published on 6 February 2009.

*Inquest in relation to the death of Diana, Princess of Wales*

2.10 In the light of some evidence given by Lord Condon (ex-Metropolitan Police Commissioner) at the inquest in relation to the death of Diana, Princess of Wales, the Coroner – Lord Justice Scott Baker – asked for my assistance as to whether there was anything in the Confidential Annex to the Report of the Interception of Communications Commissioner for 1992 which casts light on what was said in paragraph 8 of the open part of that Report. The final part of paragraph 8 states:

> *"From time to time stories are published in newspapers describing interception said to have been carried out by GCHQ or by what are usually called MI5 and MI6. Such stories are, in my experience without exception, false. They give the public an entirely misleading impression both of the extent of official interception and of the targets against which interception is directed".*

2.11 Given the unusual circumstances of this Inquest, I needed to consult the then Commissioner, Lord Bingham, and the Prime Minister on the propriety of my relaxing the normal stance taken in relation to disclosing the content of confidential documents. It was exceptional for the Interception of Communications Commissioner to comment on the contents of a Confidential Annex to a statutory Annual Report. However, in the circumstances, including the fact that there have been ministerial statements to Parliament on the subject, I think that it is right for me to have done so. The terms of a Note to the Coroner were agreed with the Prime Minister. In essence it confirmed that in the case of Diana, Princess of Wales:

- there was nothing in the 1992 Confidential Annex which in any way evidenced or constituted the basis for the 'stories' referred to in paragraph 8, and
- any breach of statutory requirements should have been reported. So far as can be ascertained there was no evidence of any reported breach.
- It was open to anyone unlawfully intercepted to lodge a complaint which would have gone to the statutory Tribunal. So far as can be ascertained the Tribunal files disclose no evidence of any relevant complaint.

2.12 I formally submitted my response to Lord Justice Scott Baker on 1 February 2008. The jury delivered its verdict on the inquest on 7 April 2008.

*ECHR decision: Liberty v. UK*

2.13 In July 2008 the European Court of Human Rights handed down judgment in Liberty v. UK. The complaint was about interception of communications, allegedly contrary to Article 8 of the Convention. The challenge related to the way in which external interception was conducted under the previous legislation, the Interception of Communications Act 1985 (IOCA). IOCA was replaced by the Regulation of Investigatory Powers Act 2000 (RIPA) which was introduced to take proper account of human rights and which contains additional foreseeability requirements. I have been advised by the Home Office that they are considering whether any additional measures are required in light of the Strasbourg judgment. I hope to be able to report on the progress of this consideration in my 2009 Annual Report.

*Briefing by the National Technical Assistance Centre (NTAC)*

2.14 Along with the Intelligence Services Commissioner, Sir Peter Gibson, I visited the National Technical Assistance Centre (NTAC) on 12 June 2008 to be briefed about their role. NTAC was established to provide technical support to public authorities, particularly law enforcement agencies and the intelligence services. It includes a facility for the complex processing of lawfully obtained protected electronic information. NTAC is the leading national authority for all matters relating to the processing of protected information into an intelligible

format and the disclosure of key material. Part III of RIPA – the investigation of electronic data protected by encryption etc – came into force on 1 October 2007 and the associated Code of Practice specifies that a public authority cannot serve any notice under section 49 of RIPA or, when the authority considers it necessary, seek to obtain permission without prior written approval of NTAC. I found the briefing very informative providing useful insights as to how I will undertake my statutory oversight role.

## Successes

2.15 It is impressive to see how interception has contributed to a number of striking law enforcement and national security successes during 2008. It has played a key role in numerous operations including, for example, the prevention of murders, tackling large-scale drug importations, evasion of Excise duty, people smuggling, gathering intelligence both within the United Kingdom and overseas on terrorist and various extremist organisations, confiscation of firearms, serious violent crime and terrorism. I have provided fully detailed examples in the Confidential Annex to this Report. I think it is very important that the public is re-assured as to the benefits of this highly intrusive investigative tool particularly in light of the on-going debate about whether or not intercept product should be used as evidence in a court of law.

## Errors

2.16 Fifty errors and breaches have been reported to me during the course of 2008. This is a marked increase when compared with the total of 24 errors and breaches reported in my last Annual Report. I consider the number of errors to be too high. By way of example, details of some of these errors are recorded below. It is very important from the point of view of the public that I stress that, apart from one instance (which was duly reported to the relevant prosecuting authority and which is referred to in paragraph 2.31 below), none of the breaches or errors was deliberate, that all were caused by human error or procedural error or by technical problems and that in every case either no interception took place or, if there was interception, the product was destroyed immediately on discovery of the error. Where breaches or errors occur, procedures are subsequently revised or strengthened in order to minimise the chances of a similar mistake being made again. The most common cause of error tends to be the simple transposition of numbers by mistake e.g., 1965 instead of 1956. The examples that I give are typical of the totality and are anonymous so far as the targets are concerned. Full details of all the errors and breaches are set out in the Confidential Annex.

2.17 The **Northern Ireland Office/Police Service Northern Ireland** reported one error where the telephone number cited on the warrant was not that of the target. The product received was deleted.

2.18 Thirteen errors were reported to me by **GCHQ** of which four are highlighted below. The first case involved the requirement to stop monitoring an overseas telephone number when that telephone was brought into the UK. GCHQ had put in place specific measures intended to identify such a change of circumstance, so that they could react accordingly and cease monitoring. Unfortunately, a lack of coordination between the analysts concerned meant that no immediate action was taken and the telephone continued to be monitored. On realising the error, interception was ceased and the incident was reported to local management; everything obtained as a result of the error was deleted. Updated working practices have been put in place to prevent a recurrence of such errors.

2.19 The second error occurred in respect of a warrant signed by the Secretary of State restricting the scope of the warrant to target one individual rather than the three requested. GCHQ knew that a warrant had been granted but only became aware of the restriction after the interception had commenced, whereupon the interception of the two unauthorised targets ceased. No transcripts or intelligence

reports were produced and everything obtained without authority was deleted from GCHQ's systems. The process for advising GCHQ of the detail of authorisations granted by the Secretary of State has been made more robust to prevent future recurrences.

2.20 GCHQ reported similar errors in two separate cases. The two incidents related to the targeting of "short" telephone numbers which resulted in the unintentional collection of calls not associated with the intended targets. The numbers targeted were 2-digits too short to be valid numbers in the jurisdiction concerned. No intelligence reports were produced, and all the collected calls were subsequently deleted. The analysts concerned have been reminded of the importance of performing number validity checks, especially for any number that appears to have fewer digits than expected. Improvements to GCHQ collection systems will also significantly reduce the risk of unintentional collection of calls to "short" numbers.

2.21 The **Security Service** reported twelve errors that were directly attributable to them. Brief details of three of these are highlighted below. In the first case the Security Service processed a modification to add a new mobile telephone number to an existing warrant. Unfortunately the submission with the new telephone number included an incorrect telephone number. This resulted in the wrong telephone number being intercepted. The number was subsequently deleted from the warrant; no product was obtained and there was no interference with privacy. Security Service officers have been reminded of the importance of carrying out thorough checks of telephone numbers added to interception warrants.

2.22 The second error involved a warrant where two digits had mistakenly been transposed when the warrant was applied for resulting in an incorrect telephone number being intercepted. None of the product from the interception had been transcribed or retained.

2.23 The third error involved the continuing interception of a target who had left the UK. A request was made for the warrant to be cancelled; however, due to an administrative error, the warrant was allowed to lapse without cancellation resulting in further interception. No communications were intercepted after the warrant lapsed. The relevant Security Service officers were reminded of the importance of suspending interception of communications with the relevant CSP as quickly as possible. A subsequent review of procedure in this area has resulted in further safeguards being put in place, aimed at avoiding this type of error in the future.

2.24. **HM Revenue and Customs (HMRC)** reported one error in respect of a revalidation document for an urgent modification. Verbal authority was given for an urgent modification to the schedules part of an existing warrant but in submitting the revalidation document to the Home Office it transpired that the 5 working day expiry date had been incorrectly calculated and the wrong expiry date had been entered on the revalidation document. The telephone number intercepted under the urgent arrangements had, therefore, been intercepted for 24 hours without the appropriate authority in place. The interception was immediately stopped and all the product destroyed. To guard against any errors of this kind recurring HMRC has enhanced its internal processes by ensuring that expiry dates are checked twice by senior officers.

2.25 The **Serious Organised Crime Agency (SOCA)** reported three errors, one of which I have highlighted. Three days after the granting of a warrant of interception, it was noted that no product was being received. A check revealed that the incorrect number had been included in the application and had been subsequently intercepted. The number intercepted was one digit out i.e., the telephone number included a "3" in the place of a "5". No product was received and the incorrect number was deleted from the warrant that same day. All the relevant staff have been reminded of the importance of double checking numbers before submitting applications for interception.

2.26 The **Secret Intelligence Service (SIS)** reported four errors. I shall give one example. The deletion of a telephone number from a warrant was authorised by a senior official in the Foreign Office. This authorisation was communicated to SIS on the following day. This was the first notification that they had received of the deletion. SIS took immediate steps to suspend collection of the telephone number, and the CSP was asked to cease the interception. The error meant that interception cover was available to SIS for a short period (no more than 36 hours) without any necessary authority in place. Fortunately, there was no traffic on the line either before its deletion from the warrant or in the short period after deletion and prior to suspension and cancellation.

2.27 The **Scottish Government** reported an error in respect of an interception warrant obtained for a police force that has had a number of renewals and modifications made to it. The most recent was an application to add a new number to the warrant. However, eight days after the modification was signed it transpired that one of the digits in the telephone number was wrong: an "8" was used instead of "2". In terms of collateral intrusion, fortunately, the number submitted in the modification application had not, according to the communications service provider, been connected and as such there was neither product obtained nor any likelihood of interception of an unknown third party. The police force concerned has revised its internal procedures to ensure no future recurrences.

2.28 The **National Technical Assistance Centre (NTAC)** reported one error where a wrong email address had been intercepted. A check on the interception after it had commenced revealed that a digit in the email address had been omitted. NTAC took immediate steps to suspend the collection and the agency receiving the product destroyed all material received relating to the unauthorised email address.

2.29 I now turn to give two examples of the nine errors made by the **CSPs**.

2.30 The first error, reported by a CSP itself, occurred in respect of product being routed to an agency other than the agency which requested the interception. Upon investigation it was discovered that this was a technical error within the CSPs system resulting in the request being allocated a case identifying number applicable to an agency which had not made the request. That non-requesting agency securely dealt with the product. The CSP operative concerned has been spoken to and will ensure full accuracy checks are made with all future case additions. The system has also been amended.

2.31 The second error, reported by the Security Service, occurred when product received from an interception indicated that the number being intercepted was different to that on the warrant and corresponding schedule served on a CSP, and that the user was not the target. This unauthorised intercept was immediately stopped and all product from the line deleted. The error was due to a technical error within the CSP and the relevant staff have been duly briefed.

2.32 No errors were reported by the **Home Office, Ministry of Defence or Metropolitan Police Counter Terrorism Command.** The error which was deliberate (and which is referred to in paragraph 2.15. above) was made by a police officer. It has no security implications, there was no invasion of privacy and because it has been reported to the relevant prosecuting authority I say no more about it in this part of my Report.

## Statistics

2.33 **Warrants (a) in force, under the Regulation of Investigatory Powers Act, as at 31 December 2008 and (b) issued during the period 1 January 2008 to 31 December 2008**

| | a | b |
|---|---|---|
| Home Secretary | 844 [929]* | 1508 [1881]* |
| The total number of RIPA modifications from 01/01/2008 – 31/12/2008 = 5344 [5577]* | | |
| Scottish Executive | 43 [28]* | 204 [145]* |
| The total number of RIPA modifications from 01/01/2008 – 31/12/2008 = 610 [367]* | | |

** For comparison purposes I have included in the parentheses warrant information for the period 1 January 2007 to 31 December 2007 as detailed in my 2007 Annual Report*

[NB: Under the Regulation of Investigatory Powers Act 2000 there is no longer a breakdown of the figures between Telecommunications and Letters.]

# Section 3: Part I Chapter II – Acquisition And Disclosure Of Communications Data

## General

3.1 The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or what was written. Certain public authorities are approved by Parliament to acquire communications data to assist them in carrying out their investigatory or intelligence function and they include the intelligence agencies, police forces, Her Majesty's Revenue and Customs, the Serious Organised Crime Agency and other enforcement agencies, such as the Serious Fraud Office and Information Commissioner's Office. Local authorities, including the Trading Standards Service, are also able to acquire a restricted set of communications data to assist them to investigate complaints made by the public.

3.2 The Act and its Code of Practice contain explicit human rights safeguards-particularly the rights of individuals to have respect for their private life and correspondence. The safeguards include restrictions prescribed by Parliament on the statutory purposes for which public authorities may obtain data; on the type of data public authorities may obtain; which senior officials within public authorities may exercise the power to obtain data; and which individuals within public authorities undertake the work to obtain data.

3.3 All public authorities, permitted to obtain communications data using the provisions of RIPA, are required to adhere to the Code of Practice when exercising their powers and duties under the Act. Generally the acquisition of communications data under the Act involves four roles within a public authority and these include the applicant, Designated Person able to authorise applications, Single Point of Contact (SPoC) and the Senior Responsible Officer. SPoCs are responsible for the development and processing of applications for communications data. They have key responsibilities under the Code of Practice and they also have a duty to ensure that the public authority acts in a lawful and informed manner. Additionally, Designated Persons must be able to act objectively and independently when approving applications for communications data and have a current working knowledge of human rights principles, specifically those of necessity and proportionality. Adherence to the Code of Practice by public authorities and CSPs is essential if the rights of individuals are to be respected and all public authorities have a requirement to report any errors which result in intrusion upon the privacy of an innocent third party.

3.4 I have a responsibility to oversee the use which public authorities have made of their powers under the Act and how they have exercised their rights and responsibilities. I am supported by a Chief Inspector and five Inspectors who are all highly trained in the acquisition and disclosure processes and the extent to which communications data may assist public authorities in carrying out their functions. A programme of inspections is drawn up with the assistance of members of my Secretariat and the Inspectors initially engage with the Senior Responsible Officer from the public authority concerned. For example, in a police force this must be at least a Superintendent or a Head of Service in a local authority.

3.5 Within every public authority each SRO must be responsible for:

- the integrity of the process to acquire communications data;
- compliance with the Code of Practice;
- oversight of the reporting of errors to me, identifying their causes and taking appropriate action to minimise the repetition of errors;
- engagement with my Inspectors and ensuring that all relevant records are produced for the inspection;
- oversight of the implementation of post-inspection Action Plans, approved by me.

3.6 Following each inspection a detailed report is prepared by the Inspector and this will outline *inter alia* what level of compliance has been achieved with the Code of Practice. Where necessary the Inspector will produce a schedule of recommendations or an Action Plan which will address all areas that require remedial action. I have sight of all of those inspection reports in order that can I properly discharge my oversight functions. The top copy of the report is sent to the head of the public authority concerned, e.g., the Chief Constable or the Chief Executive in the case of a local authority and they are required to confirm, within a prescribed time period, whether the findings are accepted and that the recommendations or action points will be implemented.

3.7 I believe that it is in the public interest that public authorities should demonstrate that they make lawful and effective use of regulated investigatory powers. My annual report should provide the necessary reassurance that the use which public authorities have made of their powers has met my expectations and those of my Inspectors, although there is no reason why a public authority cannot disclose all or part of the report which my Inspectors have prepared in relation to that authority if they so wish (whether as a result of a request made to the authority under the Freedom of Information Act or otherwise). There is provision for this in the Code of Practice, although each public authority must seek my prior approval before making any disclosure.

3.8 During the year ended 31 December 2008, public authorities as a whole made 504,073 requests for communications data to CSPs and Internet Service Providers (ISP). This figure is slightly below the number of requests which were made in the previous year. I do not intend to give a breakdown of these requests because I do not think that it would serve any useful purpose, although the intelligence agencies, police forces and other law enforcement agencies are the principal users of communications data. Later in my report I will give some indication of the extent to which local authorities use communications data as I believe that this should be placed in context. Any suggestion that a low ranking council employee may have unrestricted access to the telephone records of a member of the public is far removed from reality because a process has to be gone through first which requires the necessity and proportionality tests to be met before the necessary approval is given by a senior official.

3.9 In the same 12-month period a total of 595 errors were reported to my office by public authorities; approximately three quarters are attributable to public authorities and the remainder to CSPs and ISPs. This may seem a large number but it is very small when it is compared to the numbers of requests for data which are made nationally. I am not convinced that any useful purpose would be served by providing a more detailed report of these errors. I should add that neither I nor any of my Inspectors have uncovered any willful or reckless conduct which has been the cause of these errors. A considerable proportion of these errors were due to the incorrect transposition of telephone numbers and of course human error can never be eliminated completely. I am pleased to say more and more police forces are introducing automated systems to manage their requirements for communications data and these will inevitably reduce the number of keying errors which occur.

3.10 In October 2007, when the Code of Practice was approved by Parliament, changes were made to the arrangements under which public authorities report errors because previously they were required to notify me of any error, even though it did not result in any intrusion upon the privacy of an innocent third party. For example, if subscriber information was requested erroneously, in relation to a telephone number which did not even exist, then this would still have to be reported as an error. Additionally, certain other errors which were effectively procedural breaches of the Code of Practice also had to be reported. For example, the failure by a police force to serve a Notice upon a CSP retrospectively within one working day of an oral request being made for communications data when there was an immediate threat to life.

3.11 Accordingly I agreed to a change in the error reporting system whereby public authorities now only report errors which have resulted in them obtaining the wrong communications data and where this has resulted in intrusion upon the privacy of an innocent third party. In my judgment this change was necessary in order to highlight the most serious errors which have impacted, or potentially impacted upon individuals and to reduce unnecessary bureaucracy associated with reporting of procedural errors, particularly in relation to the police forces and law enforcement agencies, and to bring more perspective and clarity to the error reporting system. My Inspectors review these errors during the inspections to ascertain why they occurred and how recurrence can be avoided, and they work closely with the public authorities to ensure that errors are kept to the absolute minimum.

3.12 Each public authority must also keep a log of any 'recordable' errors which have occurred during the process of acquiring communications data. Generally these are procedural errors relating to non-compliance with the Code of Practice but not resulting in intrusion. I have already given one or two examples of these types of error in the preceding paragraphs. These errors have to be recorded and the record produced on inspections, as they are relevant to the inspection, and because the errors may also indicate underlying problems within the systems and processes for acquiring communications data which may require remedial attention. The frequency of 'recordable' errors may indicate to an Inspector that the overall level of compliance may not be quite as good as it should be and this is important.

## Communications data and the work of the Inspectorate during the period covered by this report.

*Police Forces and Law Enforcement Agencies*

3.13 There are 43 police forces in England & Wales; eight police forces in Scotland; and the Police Service of Northern Ireland which are all subject to inspection. Additionally my Inspectors also inspect the British Transport Police; Port of Liverpool Police; Port of Dover Police; Royal Military Police; Royal Air Force Police; Civil Nuclear Constabulary; Ministry of Defence Police; and the Royal Navy Police.

3.14 Law enforcement agencies comprise Her Majesty's Revenue and Customs; the Serious Organised Crime Agency; the Scottish Crime and Drug Enforcement Agency; United Kingdom Border Agency; and the Child Exploitation & Online Protection Centre.

3.15 All of the above mentioned public authorities, with the exception of the Civil Nuclear Constabulary, Port of Dover Police and the Child Exploitation & Online Protection Centre have now been inspected at least twice since the Inspectorate was formed about three years ago. The first inspections of the Civil Nuclear Constabulary and the Port of Dover Police took place about two years ago but since then only the latter has made one application for subscriber information and therefore there has been no requirement to conduct a second inspection.

3.16 The Child Exploitation & Online Protection Centre which operates under the auspices of the Serious Organised Crime Agency was formed in 2006 and it is dedicated to eradicating the sexual abuse of children. It was inspected for the first time in August last year and clearly communications data plays a key role in helping the Child Exploitation & Online Protection Centre work in partnership with local and international forces and Internet Service Providers (ISP) to make the Internet a safer place for our children and young people to use. For example, information from the operator of a social networking site indicated that a 13 year old girl appeared to be in a suicidal state. Prompt action by the Child Exploitation & Online Protection Centre enabled this young person to be identified through the acquisition of communications data before she attempted to take her own life.

3.17 In 2008 my team of Inspectors conducted 33 inspections of police forces and law enforcement agencies in order to complete phase 2 of the inspection programme on schedule. The areas covered by these inspections are fairly wide ranging and therefore the Inspectors work in pairs because experience shows this is more efficient and effective. Later in this section of this report I intend to give more insight into how the inspections are conducted because I believe this will give the necessary reassurance that relevant public authorities are held accountable for the way in which they exercise their powers to acquire communications data.

3.18 Generally the outcomes of the inspections were satisfactory and the Inspectors concluded communications data is being obtained lawfully and for a correct statutory purpose. One of the first aims of the inspection is to check that the recommendations or action points from the previous inspection have been implemented and this proved to be so in the vast majority of cases. As a consequence the overwhelming number of police forces and law enforcement agencies are sustaining a good level of compliance with the Act and Code of Practice. However, it came to my notice that one or two police forces had been slow to respond to the findings from the previous inspection reports and therefore I sought assurances from the Chief Constables concerned that speedy action would be taken to make the necessary improvements. Work is ongoing to achieve that end.

3.19 I am pleased to report a considerable number of police forces and law enforcement agencies are continuing to invest in automated systems for the purpose of managing their requirements for communications data. They will help to reduce the scope for errors as generally the subject telephone number or communications address only has to be entered once and then it populates itself throughout the remainder of the process. In three of the inspections, however, we found minor breaches of the Act and Code of Practice were occurring, either because of design faults or because the software had been modified inappropriately after it had been installed. In effect this meant that some of the data was not obtained fully in accordance with the law, and relevant staff in the public authorities concerned have been advised that they have a duty under the Criminal Procedure and Investigations Act 1996 to bring this to the attention of the prosecutor who will decide whether it could have an adverse effect on any criminal proceedings which are pending. In my view this is improbable because the Inspectors were satisfied that it was still necessary and proportionate to acquire the data and moreover it

could easily have been obtained lawfully if these procedural breaches had not occurred. Where necessary my Inspectors have liaised with the systems providers to make sure the automated systems are capable of operating fully within the law and the Code of Practice.

3.20 Part of the inspection entails checking whether the systems and processes for acquiring communications data are being maintained efficiently and effectively. Inherent failings and weaknesses must be identified and quickly remedied in order to minimise the risk of errors. With one or two exceptions the police forces and law enforcement agencies emerged well from this aspect of the inspection although it is important that they have the right number of well trained staff in this business area. In some instances I have been disappointed to hear that a number of the police forces have been very slow to implement change and take advantage of new streamlining procedures which were introduced when the Code of Practice was approved by Parliament in October 2007. The changes were introduced to eliminate unnecessary bureaucracy and to make sure valuable police time is not wasted. When necessary these matters are drawn to the attention of the Chief Constables in a covering letter which is issued with each inspection report. The responses have all been positive and system changes have generally now been implemented to increase efficiency and effectiveness.

3.21 My Inspectorate receives good cooperation from the CSPs who have a requirement to comply with any lawful requests for communications data which are received from the public authorities. As part of the phase 2 inspection programme the CSPs were asked to provide my Inspectors with details of the communications data they had disclosed to the public authorities during a specified period. These disclosures have been randomly checked against the records kept by the public authorities in order to verify that documentation was available to support the acquisition of the data. I am pleased to say that in all cases my Inspectors were satisfied the correct process had been applied and the data had been obtained with the approval of a designated person. I regard this as a very important check upon the integrity of the process and it is most reassuring that it has not exposed any instances of abuse or the unlawful acquisition of communications data.

3.22 During phase 2 of the inspections a great deal of emphasis has been placed upon the use which police forces and law enforcement agencies are making of the communications data which they have obtained from CSPs. They have been required to demonstrate on a case by case basis that it was necessary and proportionate to obtain the data and that it has been used for a correct statutory purpose. My Inspectors are able to assess this in two different ways and when necessary they have challenged the justifications for acquiring a specific set of data.

3.23 First, they have carried out a random examination of applications from various sectors of the business in order to judge the overall standard of the public authority. The accredited officers have a responsibility under the Code of Practice to make sure the public authority acts in a lawful and informed manner and therefore they should return any applications which do not meet the required standard. All of the police forces and law enforcement agencies which were inspected during the reporting year achieved a satisfactory standard and indeed over two thirds of them were producing good quality applications.

3.24 Secondly, in each police force or law enforcement agency the Inspectors will look in detail at two or three operations normally where communications data has been used to investigate major incidents or serious crime. They will examine a number of the applications and conduct informal interviews with senior investigating officers, applicants and analysts. If necessary they will, and often do, challenge the justifications for acquiring the data. The results of this part of the inspection have been very revealing and generally it is evident that good use has been made of the communications data as a powerful investigative tool, primarily to prevent and detect crime and disorder. It is also very apparent that

communications data plays a crucial role in the successful outcome of prosecutions and often it is the primary reason why offenders plead guilty.

3.25 I would like to highlight a few examples of how communications data is used by police forces and law enforcement agencies to investigate criminal offences. It may provide a better understanding of its importance to a criminal investigation and the following examples are based on extracts from the Inspector's reports. For obvious reasons I cannot name the individuals concerned and I do not intend to reveal the strategy for using communications data as that may inhibit the conduct of future investigations.

3.26 In the first case a group of Muslim youths were targeting people of a similar age in the ethnic Indian community and the situation became very tense when a number of youths were kidnapped off the streets and seriously assaulted. The police were called in to investigate when attempts to resolve these matters through elders in both communities met with failure. Communications data was obtained in relation to a mobile telephone which was being used by one of the suspects to orchestrate the attacks and this helped the police identify him and several of his accomplices who were arrested. In this case the communications data had been used effectively to detect and prevent crime and also indirectly to ease tensions in the community.

3.27 The second case involved a serious violent and sexual assault upon a woman who was walking her dog in the countryside. The assailant, who had no previous connections with his victim, took all of the woman's clothing and possessions, including a mobile telephone, and left her for dead. Fortunately she recovered sufficiently to summon assistance from passers-by and she was rushed to hospital. A sophisticated investigation was mounted by the police and communications data played a pivotal role in tracing the offender and bringing him to justice. He pleaded guilty when confronted with the evidence and he has been sentenced to life imprisonment, with a recommendation that he should serve at least 23 years.

3.28 Another sexual attack upon a woman had a completely different outcome. During a police investigation a man was suspected because he had previously committed offences of a similar nature. Communications data was obtained in relation to the suspect, the victim and a key witness, who was identified solely through the acquisition of the data. When the investigation team pieced all of this together they were able to cast doubt upon the victim's account of the events and eliminate the suspect completely. I highlight this example because it shows how data can help to establish innocence.

3.29 In some instances, however, errors may result in catastrophic consequences for members of the public. When that happens it is my responsibility and that of my Inspectors to investigate the circumstances and work with the public authority concerned to review their systems and processes to prevent them recurring. In this particular example the police took swift action when information from a reliable source suggested that a number of very young children were at immediate risk of falling into the hands of a paedophile ring. Subscriber information relating to an Internet Protocol (IP) Address was obtained in order to locate an address for the children but unfortunately it would appear this was not correct. The police entered the address and arrested a person who was completely innocent and further enquiries are continuing. This was a very unfortunate error and the whole process of obtaining data relating to IP addresses has been re-examined. In this case there was confusion between the Internet Service Provider and the public authority over how the data should be interpreted, particularly in relation to the critical international time zones. Better checks and balances have been put in place to help clarify the process, which includes liaison with the SPoC trainers and these should help to prevent similar errors in the future.

3.30 It is perhaps inevitable that some mistakes will be made, especially when public authorities are dealing with large volumes of communications data in complex investigations. Overall the error rate is low and indeed minute when compared to the huge number of requests which were received by the CSPs during the course of the reporting year.

3.31 The urgent oral process should only be used when a person's life might be endangered if the application procedure was undertaken in writing from the outset, or when an opportunity to make arrests or seize illicit material may be lost. It is also accepted that police forces will need to use the urgent oral process when dealing with sudden deaths, serious injuries and vulnerable persons if undertaking the application process in writing from the outset would cause unnecessary suffering and trauma to the next of kin.

3.32 Good use is being made of the urgent oral process to acquire communications data when there are immediate threats to life. Usually this applies when vulnerable or suicidal persons are reported missing but the process is also used in kidnap situations or in other crimes involving serious violence. During the inspection of the 33 police forces and law enforcement agencies last year the urgent oral process was used on over 3,300 occasions in connection with enquiries involving immediate threats to life. This is an important facility, particularly for police forces, and the interaction between relevant police staff and CSPs saves lives across the country on a continuous basis. Variable standards were found in the management of the process and the quality of the record-keeping. Some police forces achieved very good standards but others did not do as well and my Inspectors have therefore formulated and disseminated some guidance as to good practice which should ensure that there is a better level of consistency.

3.33 It is estimated that well over 80% of the requests for communications data are for subscriber information and they can only be approved by an Inspector or above. The requests for the more intrusive types of communications data must be approved at Superintendent level or above. The inspections have established that a good level of independence and objectivity exists in the approvals process and generally designated persons in police forces and law enforcement agencies are discharging their statutory responsibilities effectively. Each application must be vetted by an accredited officer before it is submitted to the Designated Person for approval.

3.34 A decision has been taken by the Association of Chief Police Officers' Data Communications Group (ACPO DCG) that the National Policing Improvement Agency (NPIA) take over responsibility for the training and accreditation of SPoC staff with effect from March 2009. I believe it is very important that all staff who are involved in the acquisition of communications data are well trained and they maintain their skills levels to the best possible standards. My Inspectorate has a very close working relationship with the ACPO DCG and senior policymakers in the Home Office who formulate policy and co-ordinate all matters relating to communications data with public authorities, industry and other external agencies such as the NPIA. In phase 3 of the inspection programme the Inspectors will be carrying out checks in this area to ensure that accredited staff are complying with the guidelines and that they attend the ACPO DCG training workshops which are delivered with the assistance of the CSPs on a regular basis.

3.35 Under the Code of Practice I have the power to direct a public authority to provide information to an individual who has been adversely affected by any willful or reckless failure in the exercise of powers under the Act. So far it has not been necessary for me to make such a direction but there is no room for complacency and each police force and law enforcement agency understands that it must strive to achieve the highest possible standards. Relevant staff in police forces and law enforcement agencies have responded positively to the inspections and they understand that they are an essential part of my oversight responsibilities. Police forces and law enforcement agencies are now well accustomed to dealing

with the legislation and the results from this year's inspections are encouraging and show steady progress.

*Security and Intelligence Agencies*

3.36 The intelligence agencies are subject to the same type of inspection methodology and scrutiny as police forces and law enforcement agencies. For the most part the work of the intelligence agencies is highly sensitive and secret, and this limits what I can say about their inspections.

3.37 During the reporting year the Security Service, Secret Intelligence Service and Government Communications Headquarters were all inspected by my Chief Inspector and one of the Inspectors. They all emerged very well from the inspections and the inspection team concluded they are achieving a good level of compliance with the Act and Code of Practice. Of all the intelligence agencies the Security Service is the largest user of communications data acquired under Part 1 Chapter II of RIPA and it has a fully automated system to manage its requirements.

3.38 Communications data is used extensively by the intelligence agencies, primarily to build up the intelligence picture about persons or groups of persons, who pose a real threat to our national security. Given the nature of their work it is perhaps unavoidable that there will be some degree of collateral intrusion into the private lives of persons who have had contact with the subjects of their investigations. However, this is recognised by the intelligence agencies from the outset and the inspections have shown that it is being managed to the best of their ability. The error rate of all the intelligence agencies is very low in comparison with the number of requests which are processed for communications data.

*Local Authorities*

3.39 There are approximately 474 local authorities throughout the UK approved by Parliament for the purpose of acquiring communications data, using the provisions of the Act. No local authority has been given the power to intercept a telephone call or any other form of communication during the course of its transmission. Local authorities may acquire communications data for the purpose of preventing and detecting crime or disorder although there are restrictions upon the types of data which they may obtain. They do not have access to traffic data which would enable them to identify the location from, or to which, a communication has been transmitted.

3.40 Generally the trading standards services are the principal users of communications data within local authorities although the environmental health departments and housing benefit fraud investigators also occasionally make use of the powers. Local authorities enforce numerous statutes and Councils use communications data to identify criminals who persistently rip off consumers, cheat the taxpayer, deal in counterfeit goods, and prey on the elderly and vulnerable. The environmental health departments principally use communications data to identify fly-tippers whose activities cause damage to the environment and cost the taxpayers large sums to recover or otherwise deal with the waste.

3.41 Local authorities are required to adhere to the Code of Practice and requests for communications data are approved at a senior level. In most cases this will be the head of the trading standards service or the heads of the environmental health departments or housing benefits sections although solicitors are also often involved. The specialist staff, who process applications for communications data, are not trained to the same standard as their counterparts in other public authorities and this has caused difficulties for some local authorities, which have not been able to attain the best possible level of compliance with the Code of Practice. I am pleased to say that the Home Office and ACPO DCG have now stepped in to provide more help to the local authorities to enable them to achieve a better level of compliance with the legislation and I will say more about this later in the report.

3.42 I am aware that some local authorities have recently been criticised for the inappropriate use of other powers which are conferred upon them under RIPA. However, no evidence has emerged from the inspections which have been conducted during the last three years to indicate communications data is being used to investigate offences of a trivial nature, such as dog fouling or littering. On the contrary it is evident that good use is being made of communications data to investigate the types of offences which cause harm to the public and to which I have already alluded in paragraph 3.40 above.

3.43 In the early part of last year a huge number of local authorities received requests under the Freedom of Information Act for disclosure of their inspection reports. The Code of Practice permits local authorities to disclose these reports but they must consult me first. If necessary certain information may be redacted from these reports as there are exemptions which may be applied under the Freedom of Information Act. For example, if the disclosure of certain information may compromise an ongoing investigation or reveal tactical methods which are used to combat crime.

3.44 I have already expressed my views on this matter in paragraph 3.7 of this report and I believe that it is in the public interest that public authorities should demonstrate they make lawful and effective use of regulated investigatory powers. This report should provide the necessary reassurance that the use which public authorities have made of their powers has met my expectations and those of my Inspectors. The huge number of requests, which were received principally from two sources in the media, placed considerable strain on the resources of my Inspectorate but nevertheless we gave full cooperation to the local authorities so that they could meet the stringent deadlines which are imposed upon them to respond to such requests under the Freedom of Information Act. All of the reports had to be reviewed before I gave my consent for the local authorities to disclose them and invariably disclosure took place with the minimum of redactions. I am hoping that in future each local authority will include a suitably redacted version of the inspection report in their publication scheme so that it can be accessed freely on the Council's website.

3.45 During the period covered by this report 123 local authorities notified me they had made use of their powers to acquire communications data. A total of 1,553 requests were made for communications data and the vast majority were for basic subscriber information. A few local authorities have used their powers to acquire service use information, including outgoing call records, in relation to the investigations which they have conducted. Indeed our inspections have shown the local authorities could often make more use of this powerful tool to investigate crimes which are relevant to their statutory responsibilities.

3.46 Virtually all of the local authorities, which have used their powers, have been inspected at least once since the legislation was introduced. The core activities of the trading standards service and environmental health teams are now centralised in a number of the larger local authorities and therefore it is easier for them to manage the process of acquiring communications data. My Inspectorate identified the largest users of communications data at an early stage and they are inspected more regularly. Regrettably a temporary shortage of staff in the Inspectorate and a requirement to prioritise other inspections meant that it was possible to conduct only one inspection of the large local authorities. It was pleasing to see the recommendations from the previous inspection had been fully implemented and the thirteen applications for communications data which had been made during a 12 month period were completed to a good standard. A number of inspections of the larger local authorities have taken place in the first quarter of 2009.

3.47 As a result of the first phase of inspections it was recognised that the majority of smaller local authorities, which make very limited or infrequent use of their powers, were struggling to achieve the best possible level of compliance with the Act and Code of Practice. Consequently a key part of the inspection

was focused upon raising awareness of their responsibilities under the Act and Code of Practice and giving advice on how they should set up or modify their systems and processes so that the data could be obtained fully in accordance with the law. The vast majority of these local authorities responded positively to the inspection reports and they assured me that the recommendations or action points would be implemented. During the reporting year one of those local authorities was inspected for a third time and it was pleasing to see that the position had been completely transformed. Approximately 33 applications had been generated since the previous inspection and they were produced to an excellent standard. However, a few other local authorities informed me that they had temporarily suspended the use of their powers until a much better level of adherence could be attained or until they could take advantage of a facility which will soon be available through the National Anti Fraud Network (NAFN). One of those local authorities was visited and the Inspector confirmed that it had not made any use of its powers since the previous inspection.

3.48 In the light of the difficulties which I have mentioned earlier in my report only seven other local authorities were inspected during the year. All of them were inspected for the first time and collectively they processed approximately 48 applications for communications data during a twelve month period. Evidence was found that some of the data was not obtained fully in accordance with the law because the correct procedures had not been followed although the Inspectors were nevertheless satisfied the acquisition of the data was justified and it had been used for a correct statutory purpose. Following these inspections the Inspectors produced detailed Action plans which are designed to bring the level of compliance up to an acceptable standard.

3.49 The local authorities reported a total of 47 errors last year and a few of these were identified during the inspections. I have not encountered any cases which would be serious enough for me to invoke the powers which I have outlined previously in paragraph 3.35 of this report.

3.50 In paragraph 3.41 of the report I alluded to the fact that the Home Office and ACPO DCG have taken positive steps to help local authorities achieve a better level of compliance with the legislation. A high proportion of local authorities subscribe to the NAFN and this organisation has been given funding by the Home Office so that it may provide a national service to its members. Members of staff from NAFN have already been trained and accredited to the same standards as their counterparts in police forces and law enforcement agencies and NAFN will shortly commence processing applications for communications data. The onus and responsibility for approving these applications still rests with the local authority concerned but NAFN will use its trained and accredited SPoC staff to quality assure them and retrieve the data from the CSPs. This is a major step change and I believe it will be of particular assistance to the local authorities which make limited or infrequent use of their powers. All local authorities which opt into the scheme will still of course be subject to inspection and my Inspectorate is liaising closely with NAFN to make the necessary arrangements.

*Other public authorities*

3.51 There are approximately 110 other public authorities which are registered for the purpose of acquiring communications data. These include the Serious Fraud Office, Independent Police Complaints Commission, Charity Commission, Royal Mail and the Medicines & Healthcare Products Regulatory Agency (MHRA), to name just a few.

3.52 A temporary shortage of staff in the Inspectorate and a requirement to prioritise other inspections meant that it was possible only to inspect a few of these public authorities during the reporting year. However, I should state that all of the public authorities in this category have been inspected at least once since the legislation was introduced and indeed some were inspected for a second

time during the reporting year. These included the Independent Police Complaints Commission, Office of the Police Ombudsman of Northern Ireland, Health & Safety Executive, National Health Service Counter Fraud & Security Management Services and the Office of the Information Commissioner.

3.53 By comparison with police forces and law enforcement agencies the above mentioned public authorities make very limited use of their powers to acquire communications data. For example, the Office of the Information Commissioner used its powers on about 37 occasions during a 12 month period although the other public authorities which were inspected for the second time had only averaged between 10 and 15 applications during the year.

3.54 Generally these public authorities acquire communications data for specialist purposes. For example, the Office of the Information Commissioner needed communications data to investigate breaches of the Data Protection Act and the Independent Police Complaints Commission made use of its powers primarily to investigate deaths in police custody.

3.55 Restrictions have been placed upon the types of data which some of the public authorities in this category may acquire. For example, the Health & Safety Executive (HSE) is not permitted to acquire traffic data, i.e., data which would enable it to identify the location from or to which a communication has been transmitted. In one instance the HSE erroneously made an application for incoming call data. This constitutes traffic data under Section 21(4)(a) of RIPA and this was not picked up when the application was submitted or approved. Subsequently a notice was served to acquire this data but fortunately the CSP spotted the error and rightly it refused to comply with the request. The Inspector was satisfied this was an isolated error, caused inadvertently, but it is worth mentioning it here because it shows how the CSPs help regulate the public authorities and ensure that only lawful requests are complied with.

3.56 With the exception of the above error the HSE managed to achieve a good level of compliance with the Act and Code of Practice. The other public authorities which were inspected in this category are also achieving good standards and they use their powers responsibly.

# Section 4: Interception in Prisons

## General

4.1 At the request of the Secretary of State I have continued to provide oversight of the interception of communications in prisons in England & Wales. This is a non-statutory role and in practice most of the inspections are conducted by my Inspectors although I have sight of every report which they produce. During this reporting year I also received a request from the Director of the Northern Ireland Prison Service to extend my non-statutory oversight responsibilities to the three prisons which operate in the province. I was happy to do so and a first inspection has already been conducted in all three establishments. They emerged quite well from the inspections although a number of recommendations were made to improve the systems and processes for conducting the interception of prisoners' communications.

4.2 The interception of prisoners' telephone calls and correspondence is permitted, and in many cases is mandatory, under the Prison Act 1952 and the National Security Framework (NSF). The NSF stipulates that any telephone call may be listened to or letter read if intelligence suggests that this is necessary and proportionate under Prison Rule 35A or YOIR 11(4). Interception is mandatory, usually in the case of Category A prisoners and prisoners who have been convicted of sexual or harassment offences, and who continue to pose a risk to children or the public. Communications which are subject to legal privilege are protected and there are also special arrangements in place for dealing with confidential matters, such as contact with the Samaritans and a prisoner's constituency MP.

4.3 All prisoners are allocated a PIN number in order that they may use the Pin phone facility to maintain contact with friends or family whilst they are in custody. They must be informed verbally and in writing that their communications are subject to interception and they must complete a contacts list which separately identifies any numbers which should be placed on the confidential side of their Pin-phone account. The telephone numbers of legal advisers will then be entered into the Pin-phone system in such a way that any calls to these numbers will automatically not be recorded. This should act as a safeguard and prevent any legally privileged conversations being monitored unintentionally but it is not totally failsafe. Following a case which received national coverage in the media last year a review was conducted and the Prison Service has introduced new measures which are designed to prevent breaches of Articles 6 and 8 of the European Convention on Human Rights. My Chief Inspector contributed to the review and the findings and good practice points which have been gathered from our inspections were taken into account.

4.4 In reality the system still relies heavily upon manual intervention and therefore no guarantee can be given that a breach will never occur in the future. Providing the prisoners and their lawyers always adhere to the rules and the prison staff apply the process diligently the risk of legally privileged communications being intercepted will be minimised. The Inspectors will of course be looking specifically at these areas when future inspections are conducted.

## Work of the Inspectorate during the period covered by this Report

4.5 There are 137 prisons in England & Wales and since the Inspectorate was formed virtually all of them have been inspected at least twice. Prisons in the high security estate are generally subject to an annual inspection but the frequency of inspections of other establishments depends on their previous level of compliance.

4.6 During the period covered by this report my Inspectors visited 89 prisons which roughly equates to two thirds of the whole estate. The inspection usually takes one working day, although in order to achieve this in the larger prisons the Inspectors work in pairs. Following the conclusion of the inspection a detailed report is prepared for me and this is sent to the Governor and relevant staff, together with a schedule of recommendations or an action plan if necessary.

4.7 Lawful monitoring carried out in accordance with published criteria can help to safeguard the public, the prison, its staff and other prisoners. It requires good practice by well trained, well led and dedicated staff. This must be supported by a sound infrastructure incorporating good quality documentation capable of being completed to the highest standard in order to provide clear and unambiguous audit trails.

4.8 Sixty of the prisons emerged well from the inspections and the overall level of compliance with the rules was satisfactory or better. Indeed the Inspectors found examples of good practice which are now firmly embedded in the systems and processes and managers and staff clearly demonstrated a commitment to achieve the best possible standards.

4.9 Regrettably serious weaknesses and failings were found in the systems and processes of the other 29 prisons which were inspected during 2008. I do not imply that prison managers and their staff are deliberately setting out to circumvent the rules because often these failings result from a lack of equipment and resources to conduct the interception efficiently and effectively, especially when large numbers of prisoners need to be monitored because they are considered a risk to children or are subject to harassment restrictions. The monitoring of prisoners for public protection purposes must be geared to risk and to the resources that are available to conduct the monitoring in each prison. In my judgment each establishment must

try to adopt the most tenable position it can, given that there may be a large number of individuals who are subject to safeguarding children procedures or harassment restrictions. In some instances this may not always be the best position but good evidence should be created to show that the risk factors have been taken into account, as far as possible, and that it is all that can be achieved in the prevailing circumstances.

4.10 Quite often these failings occur because a good joined up approach does not exist between staff in Security and the Offender Management Unit (OMU). Generally the staff in the OMU will have responsibility for identifying and risk assessing prisoners who they perceive to be in need of monitoring, and authorisations will be obtained for this purpose. The Security staff are then expected to monitor all the communications of these prisoners even though the targets which they have been set are neither realistic nor attainable. Fortunately my Inspectors have not found any evidence of harm to children or members of the public who need to be protected from these prisoners. It may be the risk assessment process is not being applied as robustly as it could be. Nevertheless there are a number of extreme cases where the Inspectors found a complete breakdown in the procedures for monitoring prisoners for public protection purposes and this must be a cause for concern.

4.11 The inspections have also revealed that certain prisons do not have the capacity to monitor prisoners who pose a real threat to their good order and security and this is a cause for concern. The smuggling of drugs and illicit mobile telephones are serious problems for most prisons, irrespective of their security status, and if a serious incident were to occur, which could have been prevented through the gathering of intercept intelligence, then prison managers and staff could find themselves in an indefensible position. Regrettably my Inspectors have had to emphasise this point in a number of their reports. For example, in one large Category B local prison which holds approximately 1400 prisoners, no prisoners were subject to targeted monitoring although over 110 illicit mobile telephones had been seized in the establishment during a period of about 12 months.

4.12 Over a year ago my Chief Inspector and I met the Director General of the Prison Service to review the outcomes from the various inspections and this was very useful. The Inspectorate has an excellent working relationship with the National Intelligence Unit and a new strategy for intercepting prisoners' communications was developed in response to the findings of the inspections. In my previous report I mentioned that the Prison Service intended to trial the new strategy in a number of prisons but progress has been slow. I understand that the pilot exercise has now been authorised and that it should commence in the near future. Hopefully the results will be available for the Secretary of State and Director General to consider later this year.

4.13 Despite the difficulties which are being experienced in some of the prisons I am encouraged by the fact that more and more of the Governors are ensuring that the recommendations from the inspections are implemented. The work which the Governors and their staff have put in to improve the systems and processes is commendable and much appreciated by me and the Inspectors. It is also rewarding when one hears that the intelligence yield has increased, and that this has made the establishment a much safer place for prisoners and members of staff.

# Section 5: Other Matters

## Foreign and Commonwealth Office and Northern Ireland Office warrants

5.1 In paragraphs 31 – 33 of my Annual Report for 2006, I set out the reasons for not disclosing the number of warrants issued by the Foreign Secretary and the Secretary of State for Northern Ireland in the main part of the Report. I take this opportunity to emphasise again the reasoning behind this decision.

5.2 This practice is based on paragraph 121 of the Report of the Committee of Privy Councillors appointed to inquire into the interception of communications and chaired by Lord Birkett. The Birkett Committee thought that public concern about interception might to some degree be allayed by the knowledge of the actual extent to which interception had taken place. After carefully considering the consequences of disclosure upon the effectiveness of interception as a means of detection, they decided that it would be in the public interest to publish figures showing the extent of interception, but to do so only in a way which caused no damage to the public interest. They went on to say:

> *"We are strongly of the opinion that it would be wrong for figures to be disclosed by the Secretary of State at regular or irregular intervals in the future. It would greatly aid the operation of agencies hostile to the state if they were able to estimate even approximately the extent of the interceptions of communications for security purposes."*

5.3 Like my predecessors I am not persuaded that there is any serious risk in the publication of the number of warrants issued by the Home Secretary and the First Minister for Scotland. This information does not provide hostile agencies with any indication of the targets because as Lord Lloyd said in his first Report published in 1987 "the total includes not only warrants issued in the interest of national security, but also for the prevention and detection of serious crime." These figures are, therefore, set out in paragraph 2.32 of this Report. However, I believe that the views expressed in Lord Birkett's Report still apply to the publication of the number of warrants issued by the Foreign Secretary and the Secretary of State for Northern Ireland. I also agree with the view of my predecessor, Lord Nolan, that the disclosure of this information would be prejudicial to the public interest. I have, therefore, included them in the Confidential Annex to this Report.

## Safeguards

5.4 Sections 15 and 16 of RIPA lay a duty on the Secretary of State to ensure that arrangements are in force as safeguards in relation to the dissemination, disclosing, copying, storage and destruction etc., of intercepted material. These sections of the legislation require careful and detailed safeguards to be drafted by each of the agencies and for those safeguards to be approved by the Secretary of State. This has been done. My advice is sought on proposed amendments to the safeguards when they are updated in light of technical and administrative developments. During the period of this report I saw and commented on the revised handling arrangements for the Metropolitan Police Service Counter Terrorism Command. I also reviewed and approved GCHQ's Compliance Documentation, which is readily available to all who work in GCHQ.

# Section 6: The Investigatory Powers Tribunal

## Statistics

6.1 The Investigatory Powers Tribunal (the Tribunal) was established by section 65 of RIPA. The Tribunal came into being on 2 October 2000 and from that date assumed responsibility for the jurisdiction previously held by the Interception of Communications Tribunal, the Security Service Tribunal and the Intelligence

Services Tribunal and the complaints function of the Commissioner appointed under the Police Act 1997 as well as for claims under the Human Rights Act. The President of the Tribunal is Lord Justice Mummery with Mr. Justice Burton acting as Vice-President. In addition, four senior members of the legal profession served on the Tribunal for the whole of 2008, one member having stepped down at the end of February 2008.

6.2 As I explained in paragraph 39 of my Annual Report for 2006, complaints to the Investigatory Powers Tribunal cannot easily be "categorised" under the three Tribunal systems that existed prior to RIPA. Consequently, I am unable to detail those complaints that relate to the interception of communications that would previously have been considered by the Interception of Communications Tribunal. I can only provide the information on the total number of complaints made to the Investigatory Powers Tribunal. The Tribunal received 136 new applications during the calendar year 2008 and completed its investigation of 70 of these during the year as well as concluding its investigation of 32 of the 41 cases carried over from 2007. 75 cases have been carried forward to 2009.

6.3 In 2007 the Tribunal received 66 new applications and completed its investigation in relation to 31 of them, so in 2008 the workload increased by over 100%. Despite the increase in the disposal rate the inevitable result has been an increase in the time taken to deal with applications, given that there has been no increase in the size of the Tribunal or in the size of its support staff, and the trend has continued, so consideration should be given to the question of whether increasing delays in dealing with applications are acceptable, and if not what can be done to assist, given the time that it takes to recruit suitable staff and arrange security clearance.

## Assistance to the Tribunal

6.4 Section 57(3) of RIPA requires me to give all such assistance to the Tribunal as the Tribunal may require in relation to investigations and other specified matters. My assistance was not sought by the Tribunal during 2008.

## Determination made by the Tribunal in favour of two separate complainants

6.5 During 2008 the Investigatory Powers Tribunal made two determinations in favour of two separate complainants. These are the second and third occasions that the Tribunal has upheld a complaint, the first being recorded in my predecessor, Sir Swinton Thomas's, final Annual Report for 2005-2006. On the grounds of confidentiality, the Investigatory Powers Tribunal Rules 2000 prohibit me from disclosing specific details about the two complaints, but it is sufficient to say that the conduct complained of was not authorised in accordance with the relevant provisions of RIPA. In its ruling in the first case the Tribunal ordered payment of an award of compensation to the complainant, as provided by section 67(7) of RIPA, though the respondents were not required to destroy the relevant records. In the second case, no award of compensation was made but the respondents were ordered to destroy the evidence of the unauthorised conduct.

# Section 7: Conclusion

7.1 As I said in my previous Reports, the interception of communications is an invaluable weapon for the purposes set out in section 5(3) of RIPA. It has continued to play a vital part in the battle against terrorism and serious crime, and one that would not have been achieved by other means. The task of the agencies working in this field has become, and is becoming ever more, technical and difficult as a result of the greater sophistication of terrorists and criminals. I am satisfied that Ministers and the intelligence and law enforcement agencies carry out the work, which I am required to consider, diligently and in accordance with the law.

7.2 I would also like to say that my work would be impossible without the generous support of the small secretariat which works with me, with the Intelligence Services Commissioner, and with the Investigatory Powers Tribunal. They, and the inspectors to whom I have referred, have all done excellent work, and I am very grateful to them.

7.3 Finally I would like to draw your attention to the Wilson Doctrine. My predecessor could find no justification for it, and neither can I. The statute and the oversight regime exist to ensure that, so far as is reasonably practicable, no-one's privacy is invaded without proper authorisation given because there seems to be good reason to take that step. Why should Members of Parliament not be in the same position as everyone else? At a time when other parliamentary privileges are under review it might be appropriate for this one to be swept away.

Printed in the UK by The Stationery Office Limited
on behalf of the Controller of Her Majesty's Stationery Office
ID 6211871 07/09 433849 19585

Printed on Paper containing 75% recycled fibre content minimum.


Published by TSO (The Stationery Office) and available from:

**Online**
**www.tsoshop.co.uk**

**Mail, Telephone Fax & E-Mail**
TSO
PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries 0870 600 5522
Order through the Parliamentary Hotline Lo-Call 0845 7 023474
Fax orders: 0870 600 5533
E-mail: customer.services@tso.co.uk
Textphone: 0870 240 3701

**The Parliamentary Bookshop**
12 Bridge Street, Parliament Square,
London SW1A 2JX
Telephone orders/ General enquiries: 020 7219 3890
Fax orders: 020 7219 3866
Email: bookshop@parliament.uk
Internet: http://www.bookshop.parliament.uk

**TSO@Blackwell and other Accredited Agents**

**Customers can also order publications from**
TSO Ireland
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401