

IN THE UNITED STATES DISTRICT COURT  
FOR THE EASTERN DISTRICT OF VIRGINIA  
RICHMOND DIVISION

NTP, INC.,

Plaintiffs,

v.

RESEARCH IN MOTION, LTD.

Defendant.

Civil Action No. 3:01CV767

**THE UNITED STATES' STATEMENT OF INTEREST**

Pursuant to 28 U.S.C. § 517<sup>1</sup>, the United States files this Statement of Interest and seeks leave to supplement its Statement in this case to permit it to assess the scope of the government's interest in this case prior to this Court's consideration of any motion by plaintiff to enjoin the use of any BlackBerry devices, or reinstatement of the final injunction, as set forth in this Court's Order of August 5, 2003. The United States is not a party to this litigation.

**I. INTRODUCTION**

The United States (government) is a major user of BlackBerry™ devices and technology to allow its employees to access e-mail, and to send messages, when they are away from their offices and do not have computer access to their agencies' networks. As set forth below, and

---

<sup>1</sup> 28 U.S.C. § 517 provides that "any officer of the Department of Justice, may be sent by the Attorney General to any state . . . to attend to the interests of the United States in a suit pending in a court . . . of a State, or to attend to any other interest of the United States."

acknowledged by NTP, an injunction entered pursuant to 35 U.S.C. § 283 cannot enjoin use of a patented invention by the federal government because the exclusive remedy for any such unauthorized use of a patented invention is the award of compensation pursuant to 28 U.S.C. § 1498(a). However, in the formulation of any injunction, it is imperative that some mechanism be incorporated that permits continuity of the federal government's use of BlackBerry™ devices and establishes some procedure for identifying those devices that lie outside the scope of any injunction entered in this action.

As also set forth below, the federal government may have a further interest in this case to the extent that it is vital for it to be able to communicate in real-time with private parties, including government contractors, through BlackBerry™ devices. The government is currently assessing the extent of its interest in such communications, and the extent to which the public interest would be impaired by the award of any injunctive relief to NTP.

## **II. STATEMENT OF THE CASE**

This is a private patent infringement action filed by NTP, Inc. (NTP) against Research in Motion, Ltd. (RIM). At issue currently is the infringement of five patents relating to electronic mail transmission. On August 2, 2005, the Federal Circuit, in a revision of an earlier opinion, affirmed this Court's claim constructions, except for that of a limitation relating to an "originating processor," vacated this Court's decision and remanded for further proceedings to take into account the modified claim construction. *NTP, Inc. v. Research in Motion, Ltd.*, No. 03-1615, slip op. at 48 (decided August 2, 2005). It further held that none of the process claims could be infringed by the operation of the RIM system because one of the steps claimed to correspond to a limitation of those claims occurred outside of United States territory. It,

however, affirmed this Court's decision that claims drawn to a system could be held infringed despite the fact that a relay station was located in Canada. *Id.* at 73. The mandate was issued on October 21, 2005.

### III. ANALYSIS

#### A. Any Injunction Must Provide A Workable Procedure For Ensuring That Government Users Are Able To Continue To Use BlackBerry™ Devices And Products

Pursuant to 35 U.S.C. § 283, a district court “*may grant* injunctions in accordance with the principles of equity. . . .” (emphasis added). However, injunctive relief awarded in a private patent infringement suit does not prevent the manufacture or use of a patented invention by or for the government because the remedy against the government is strictly compensatory. *Trojan, Inc. v. Shat-R-Shield, Inc.*, 885 F.2d 854, 856-57 (Fed. Cir. 1989). Recognizing this, NTP has stated to the Federal Circuit:

As a matter of law, injunctions cannot apply to the federal government – a legal point on which RIM has attempted to mislead the district court. As for state and local government, NTP unequivocally stated to the District Court that any issued injunction would not apply to such users.

NTP's Response in Opposition to RIM's Motion to Stay Issuance of the Mandate Pending Filing and Disposition of Petition for Writ of *Certiorari*, filed October 18, 2005, at 12 n.2.<sup>2</sup> Indeed, in NTP's Proposed Scheduling Order, filed November 1, 2005, it stated that it will propose an injunction with exceptions for federal, state and local governments, as well as first responders, such as the American Red Cross. *Id.* at 5.

---

<sup>2</sup> State governments enjoy an Eleventh Amendment immunity from patent infringement actions in federal courts. *Florida Prepaid Postsecondary Educational Expense Board v. College Savings Bank*, 527 U.S. 627 (1999).

Despite NTP's concession, there appear to be significant issues with the manner in which any injunction is phrased, and implemented. The previously entered injunction broadly enjoined "RIM . . . and all those in active concert or participation with RIM. . . .from indirectly or directly making, using, offering to sell, or selling within the United States or importing into the United States" a number of BlackBerry™ handheld devices, along with the Corporate, ISP and Desktop versions of its Redirector software, as well as offering wireless e-mail service on any of three networks, including the GPRS network. Final Order, entered August 5, 2003, at ¶ 3a. The language of this injunction would literally prohibit RIM from providing the services that would be essential for the federal government, as well as state and local governments, to continue their use of the BlackBerry™ devices. That would amount to a *de facto* injunction against the government's use of BlackBerries, contrary to the *Trojan* decision.

Moreover, there does not appear to be a simple manner in which RIM can identify which users of BlackBerries are part of the federal government, so that e-mail directed to them can be relayed through the BlackBerry™ system. First, according to RIM, it does not maintain a listing of e-mail addresses associated with government users, so that one might attempt to segregate addresses that end in .gov or .mil. (Dec. Of Clark, Ex. A at pp. 2-3).<sup>3</sup> Rather, RIM relies upon a PIN (Personal Identification Number) as a means of uniquely identifying every BlackBerry™ device. Thus, there is no simple way in which federal government users can be easily identified

---

<sup>3</sup> The declaration of David Clark, Director of BES Technology at RIM, which includes a Memorandum describing the information used in relaying e-mail transmissions to and from BlackBerry™ devices, is attached hereto as Exhibit 1. Defendant has attached a .pdf version of this declaration bearing the signature of David Clark, and respectfully requests leave to substitute the original signed copy of the declaration once it is received.

to assure that their service is not being cut off along with commercial users. The same would apply to state and local governments, and any other authorized users.

One possibility for implementing the exception for federal government users recognized by NTP, and mandated by case law, would be to develop a database containing a “whitelist” of devices used by the federal government, as well as any other users who are excepted from the scope of any injunction. This raises some substantial challenges that cannot be instantly surmounted. In order to be useful, and to avoid inaccuracies in transferring information, any whitelist should take the form of an electronic database. This requires some determination to be made by RIM and government users as to the appropriate format in which to provide this information so that it can be incorporated into a usable database maintained by RIM. Next, the particular government entities who are authorized to transmit this information must be identified to avoid duplicate, and possibly inaccurate, data from being transmitted by multiple government offices or employees. (See, Dec. Of Clark, Ex. A at p. 4). Additionally, there would probably have to be a procedure for each agency to certify to this Court that it has transmitted a list of PINs and associated information that represents devices that are being used by the federal government, in order to provide a mechanism for assuring that RIM did not overstep the bounds of any injunction in implementing a whitelist.

After some decision is made as to a proper format, and authorization process, for providing whitelist information to RIM, each federal agency would need to compile an electronic list of the PINs and associated information for each BlackBerry™ used by its employees in their official capacity. Since the federal government does not maintain any central agency for purchasing and deploying BlackBerry™ devices, the procedure for supplying information to

identify government-owned BlackBerry™ devices may require a time-consuming inventory of every agency within the federal government, including the legislative branch and the judicial branch, in order to assure that service to those devices is not terminated as part of any injunction.<sup>4</sup> We are presently assessing the scope of the burden, and amount of time, that would be required.

Finally, RIM would need to incorporate this information into its database, so that the federal government's communications, which include a raft of time-sensitive official communications, are not disrupted by any injunction. This procedure would become more complicated, and prone to error, when state and local government users, essential government contractors, and Non-Governmental Organizations, such as the American Red Cross, are added to the whitelist of authorized users.

Thus, the government has a substantial interest in assuring that the terms of any injunction awarded to NTP incorporate a reasonable procedure to permit identification of government users so that the federal government's right to continue its use of BlackBerry™ devices is not rendered a nullity.

It is further worth noting that the five patents involved here are all undergoing re-examination by the Patent and Trademark Office (PTO). Given the potential complexity and expense involved in inventorying the government's BlackBerry™ devices, it may make sense to stay any consideration of the reimposition of the injunction for at least 90 days, during which

---

<sup>4</sup> After recognizing that BlackBerry™ devices permitted emergency communications during times when other communications systems were inoperative, Congress issued them to every member. See Congressional Research Service, *Congressional Continuity of Operations (COOP): An Overview of Concepts and Challenges* CRS-7 to CRS-8 (updated February 3, 2004).

time the PTO may issue a final decision regarding the re-examination. This would permit the government to undertake a government-wide inquiry to determine the feasibility, expense and time requirements of providing the information required for a whitelist of users who are not subject to any injunction, by NTP's own admission.

There may also be a substantial public interest that would be impaired by enjoining commercial use of BlackBerry™ devices. The government needs additional time, however, to assess such further public interest. Staying consideration of reimposition of any injunction for 90 days would permit the government to consider such additional public interest.<sup>5</sup>

### **III. CONCLUSION**

The United States has a considerable interest in this action, to assure that its use of BlackBerry™ devices and software, which falls outside of the scope of any injunction that may be entered by this Court, is not impeded and that the public interest is not substantially harmed by any injunctive relief. In order to protect that interest, the government asks that it be served with copies of all filings in this case bearing on any injunctive relief, and that it be permitted to present evidence and arguments, and make further filings directed toward that issue.

DATED this \_\_\_ day of November, 2005.

Respectfully submitted,

PAUL J. McNULTY  
UNITED STATES ATTORNEY

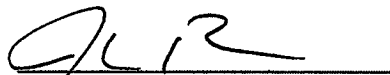
---

<sup>5</sup> For example, it is quite possible that there is a strong public interest in being able to convey health or public emergency warnings to non-governmental users who have BlackBerry™ devices, and can take immediate action in response to such information.



Robert P. McIntosh  
Assistant United States Attorney  
Virginia Bar No. 66113  
600 East Main Street, Suite 1800  
Richmond, Virginia 23219  
Telephone: (804) 819-7404  
Facsimile: (804) 819-7417

PETER D. KEISLER  
Assistant Attorney General  
Civil Division



JOHN FARGO  
New York Bar No. 2986966  
Director, Commercial Litigation Branch  
Civil Division  
Department of Justice  
Washington, DC 20530  
Tel: (202) 514-7223  
Fax: (202) 307-0345



**UNITED STATES DISTRICT COURT  
EASTERN DISTRICT OF VIRGINIA  
RICHMOND DIVISION**

**NTP, INC.**

**Case No. 3 01 CV 767**

**Plaintiff**

**v.**

**Judge James R. Spencer**

**RESEARCH IN  
MOTION, LTD.,**

**Date:**

**Time:**

**Defendant**

**Place:**

**Trial Date:**

**DECLARATION OF DAVID CLARK ADOPTING  
BLACKBERRY WHITE-LISTING MEMORANDUM**

I, David Clark, hereby declare:

1. I am employed by Research In Motion, Ltd. ("RIM") in the capacity of Director, BES Technology. I have a Ph.D. in Computer Science from the University of Waterloo and a B.Sc., combined Honours, Mathematics and Computer Science from the University of Victoria. I have been employed at RIM for five and one-half years.
2. In my capacity as Director, BES Technology, I am fully knowledgeable of the manner in which the BlackBerry systems and system hardware and software function, including the manner in which messages are transmitted through the systems and the manner in which the identity of users can be determined.
3. I have prepared a description of the information that is available to RIM about its end-customers. This memo is attached hereto and made a part hereof as "Exhibit A" as if fully incorporated herein. The memo consists of six numbered pages the fifth of which is identified as "Appendix A".
4. The memo discusses the technical issues that would surround the creation of a "white list" of BlackBerry users who would be authorized to continue operation in the face of a possible court injunction blocking operation of BlackBerry service in the United States to other users.

I declare under the penalty of perjury under the laws of the United States that the foregoing is true and correct. Executed on November 8, 2005.

  
\_\_\_\_\_  
David Clark

# EXHIBIT A

## BlackBerry White-Listing

This memo summarizes the information provided to RIM about its end-customers. In addition, it discusses technical issues surrounding the creation of a “white list” of BlackBerry users authorized for continued operation in the face of a possible court injunction blocking operation of the BlackBerry service in the U.S.A.

### *Identity Information Passed to Research In Motion*

Research In Motion obtains device and BES information through several paths:

1. Handheld Provisioning by the Carrier,
2. Handheld Contact with RIM’s Network Operations Center (NOC),
3. BES connection with RIM’s NOC,
4. Contact Centre interactions, and
5. Email/Data transmissions.

In each case, insufficient information is passed to Research In Motion to allow reliable and authenticated determination of the end customer or organization.

#### Handheld Provisioning by the Carrier

When authorizing RIM to bill the carrier for providing BlackBerry service to a handheld, the carrier provides some of the following pieces of information

- Handheld PIN,
- Handheld IMEI (GSM, IDEN) or ESN (CDMA),
- Subscription Information (IMSI, ICCID, and possibly MSISDN), and
- Service types (BES, BIS, Paging, Browsing,...).

The exact information provided varies by carrier. Note that the subscription information does not identify the subscriber to RIM but instead refers to a relationship the carrier maintains with the customer. For GSM, the values are associated with the “smart card” supplied to a user by the carrier to activate a phone (SIM). RIM uses this information to determine which carrier has agreed to pay for providing BlackBerry service to a handheld. Carriers and their resellers do not provide RIM with the identity of their customers as part of the provisioning process.

#### Handheld Contact with RIM’s NOC

BlackBerry contacts RIM’s NOC upon its first roaming on to a carrier in order to download configuration information relevant to that carrier. During this “registration” process, it transfers the following information:

- Home Network Provider Code (network type and carrier identity),
- Active Network Provider Code (network type and carrier identity),
- Carrier subscription information (IMSI, ICCID, MSISDN (phone number) - if known, EFGID1&2 if applicable),
- Handheld information (type, PIN, IMEI or ESN),

- Software version information (OS/Platform version, Applications version),
- Under Version 4 registration, encryption key to be used for later authentication challenges, and
- SRP IDs of any routable services on the device, including indication of desktop redirector use.

This information is used by RIM to verify the billing relationship and determine the correct configuration to download. The information included here is not sufficient for RIM to identify the actual end-user or their organizational affiliations.

So long as the BlackBerry maintains its connection to the Relay no additional identifying information is given to RIM; however, when a new connection is established or key items change the registration information may be re-sent.

### **BES connection with RIM's NOC**

When the BlackBerry Enterprise Server connects to RIM's NOC, it transfers the following information

- SRP ID and code (authorization for BES use)
- BES version information
- Underlying mail service type
- Reconnection reason (connection loss, crash, machine reboot...)

The source IP address of the connection is also carried in these transactions at the IP layer. At this time, the BES does not supply user identity information to the NOC.

### **Contact Centre Interactions**

RIM's contact center/technical support groups will obtain contact information for those customers with which it has a relationship. For customers with a paid-support contract this information will include BES SRP ID information.

### **Email/Data Transmissions**

Finally, the following information is passed in the unencrypted portion of the email payload that passes through RIM's NOC:

- 1) The SRP ID of the BES
- 2) The PIN of the BlackBerry
- 3) A code that indicates the type of message in the packet
- 4) Encryption identification and headers for decryption
- 5) Transaction number

The IP addresses of both endpoints (NOC components and handheld) are also carried at the IP layer. Note that the IP address of the handheld is a private IP address only valid in the context of the particular carrier connection to RIM and is only valid for a period of time. A more detailed overview of the information flow for email is contained in Appendix A.

### ***NOC Support for a White List***

RIM authorizes and tracks its service on the basis of two unique identifiers

- SRP ID for the BES
- PIN for the handheld

While other device identifiers are available, they are generally translated to the PIN for service management.

Therefore any white list would need to consist of a list of SRP IDs and a list of PINs for those endpoints authorized to continue to receive BlackBerry service. If an injunction was issued and a white list of users excluded from its effect is to be supported, RIM would need to create mechanisms to abide by the injunction but still allow the white-listed servers and handhelds to operate. In addition, efforts would have to be taken to ensure that, to the extent possible, devices not located in the United States would not be incidentally turned off since they would not be subject to any injunction.

RIM is not in a position at this time to supply a committed schedule to perform the analysis and work needed to exclude a specified white list of users from the affect of an injunction should one issue. This would require the establishment of a model under which all traffic from all devices in the United States other than those included a white list is blocked. RIM is continuing to evaluate the alternatives and associated design risks and will provide additional information as it becomes available. RIM believes that much of the implementation effort could be conducted in parallel with the efforts of any white listed organizations to provide RIM with the white lists. Once the development work is completed, at least an additional two to three weeks would be required for testing and deployment. Deployment would include both enabling the changes at RIM as well as any changes required at the customer sites. However, having said all this it is important to note that RIM is not currently in a position to comment on the commercial viability, either short or longer term, of RIM or the carriers continuing to providing service and support in the United States for a drastically reduced customer base.

### ***Determining Authorized Users***

Any white list for BES and handhelds would be defined on an organizational basis. There is currently no reliable organizational or personal information available to Research In Motion on which to base the construction of the white list. Therefore, any such process would require the creation of new systems for the collection and maintenance of the white list. If the court were to authorize certain organizations to continue receiving BlackBerry service, those organizations would be expected to gather the SRP IDs and PINs for their servers. These organizations would be required to aggregate this information (with appropriate authorizations) and provide the resulting white list to RIM. It is not currently clear how RIM would manage the ongoing receipt of information from what may end up being thousands of independent agencies with varying levels of technical expertise and sophistication. At minimum, RIM would need to develop an electronic data interchange system to facilitate the initial transfer and ongoing maintenance of these records.

In addition, it is not sufficient to just gather the initial information. Whatever processes are put in place must be adequate to handle the timely addition of new handhelds and the removal of handhelds no longer under authorized use.

Based on NTP's comments to date, it would appear that information would have to be gathered from the following groups:

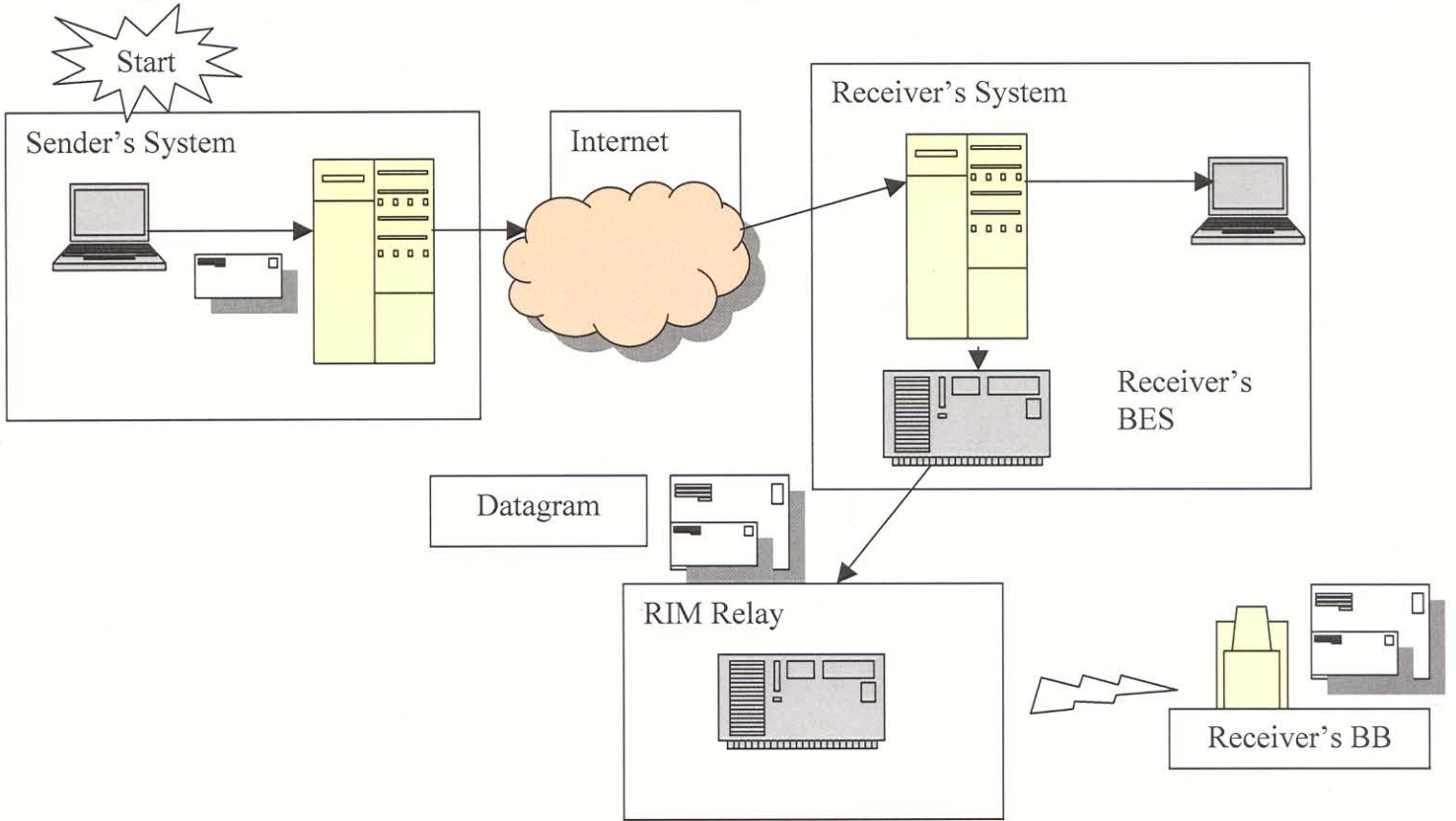
- Federal government agencies
- Authorized government contractors
- State government agencies,
- Municipal employers including emergency services, and
- Certain NGO employers.

The scope included by 'government' is not clear at this time. RIM is not able to state the volume of PINs that would need to be collected but currently estimates that there are between 50,000 and 200,000 PINs associated with government users. The number of BES is also unknown at this time but likely exceeds 1000 based on the estimates of the number of users. Clearly the amount of information gathered and the coordination required will increase as the number of authorized organizations increases. There would also have to be processes in place to ensure that RIM had the assurances it requires that the PINs it is provided with are associated with devices allocated to white listed users.

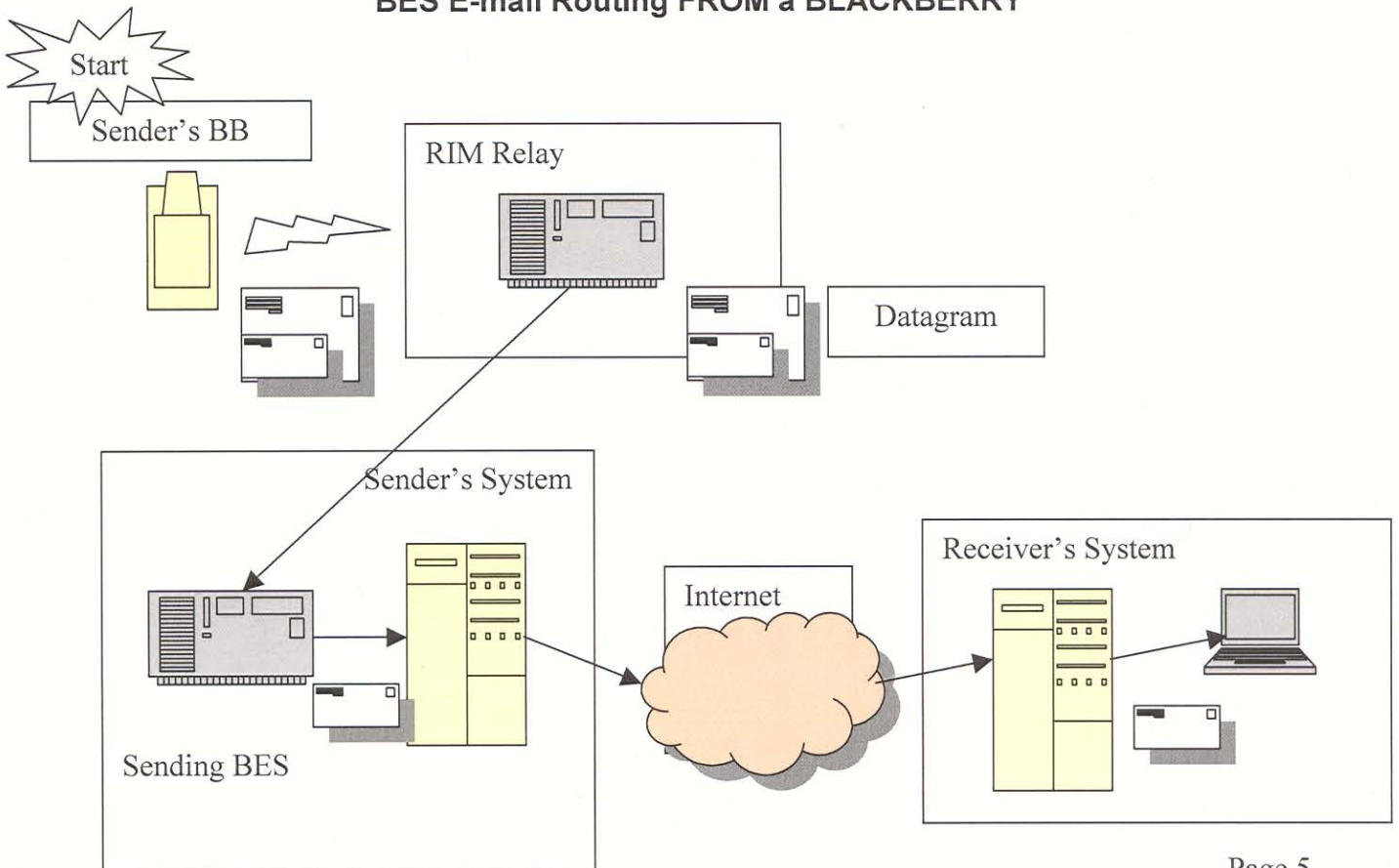
If the government wishes to explore the feasibility of this framework further, we recommend that the government explore the following requirements:

- Finalization of the definition of the government agencies, employees and contractors it wishes exempted from any injunction
- Creation of a central database of authorized administrators and authentication information
- Creation of tools for those administrators to maintain a list of BES and handhelds at the central site for each of their BES (RIM may be able to provide advice on setting up these processes)
- Setting up processes to upload the white listed BES and handhelds to RIM on an ongoing basis.

# Appendix A: BES E-mail Routing TO a BLACKBERRY



# BES E-mail Routing FROM a BLACKBERRY



### BES e-mail routing to a BlackBerry

The first contact with Relay is through the Receiver's BES.

When the e-mail first hits the Receiver's BES the BES looks up the receiver's PIN. The email is compressed and encrypted by the BES. A RIM header is added and it contains the following unencrypted information (as well as some non-material data):

- 1) The SRP ID of the receiver's BES
- 2) The PIN of the receiver's BB
- 3) A code that indicates the type of message in the packet
- 4) Encryption identification and headers for decryption
- 5) Transaction number

The Relay can extract information from only the headers due to the encryption of the actual email message data.

### BES e-mail routing from a BlackBerry

The first contact with the Relay is through Sender's BlackBerry.

The e-mail is generated on the sender's BlackBerry. Before transmitting the e-mail, the sender's BlackBerry compresses and encrypts the email. A RIM header is added and it contains the following unencrypted information:

- 1) The SRP ID of the sending BES (ie. the BES associated with the device)
- 2) The PIN of the sending device
- 3) A code that indicates the type of message in the packet
- 4) Encryption identification and headers for decryption
- 5) Transaction number

This information is transmitted by UDP/IP to the Relay. The IP routing protocols includes the source IP address. As such, it is possible to obtain an IP address for the BlackBerry. Such an IP address is, in general, only valid within the context of the specific Relay connection to the carrier. This is a private IP address for the device which is temporarily and randomly assigned for a given connection. From it, RIM can deduce no user information beyond what is already set out herein

The Relay can extract information from only the headers due to the encryption of the actual email message data.



**CERTIFICATE OF SERVICE**

I certify that a true copy of the foregoing **THE UNITED STATES' STATEMENT OF INTEREST** was sent to the undersigned counsel by facsimile and first class mail, postage prepaid on this 8<sup>th</sup> day of November 2005:

Jack E. McLard  
Maya M. Eckstein  
HUNTON & WILLIAMS  
Riverfront Plaza, East Tower  
951 East Byrd Street  
Richmond, VA 23219-4074  
Fax: (804) 344-7999

Christopher V. Mills  
WILEY, REIN & FIELDING, LLP  
7925 Jones Branch Drive, Suite 6200  
McLean, VA 22102  
Fax: (703) 905-2820

James H. Wallace, Jr.  
John B. Wyss  
Gregory R. Lyons  
Floyd B. Chapman  
Scott E. Bain  
WILEY, REIN & FIELDING LLP  
1776 K Street, N.W.  
Washington, DC 20006  
Fax: (202) 719-7049

Attorneys for Plaintiff

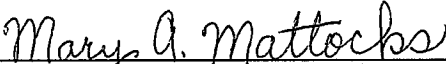
Robert M. Tyler  
David E. Finkelson  
McGUIREWOODS LLP  
One James Center  
901 E. Cary Street  
Richmond, VA 23219  
Fax: (804) 225-5377

Henry C. Bunsow  
HOWREY LLP  
525 Market Street  
San Francisco, CA 94105  
Fax: (415) 848-4999

David W. Long  
Mark L. Whitaker  
HOWREY LLP  
1299 Pennsylvania Avenue  
Washington, DC 20004  
Fax: (202) 318-8464

Robert C. Laursen  
HOWREY LLP  
2020 Main Street  
Irvine, CA 92614  
Fax: (949) 721-6910

Attorneys for Defendant

---

Mary A. Mattocks  
Staff Assistant, Department of Justice  
(202) 514-6881