UAE, BlackBerry Fight Highlights Global Internet Freedom Risks

by CDT Staff
August 4, 2010

The New York Times recently reported [1]that the United Arab Emirates is preparing to suspend the use of BlackBerry mobile services unless Research in Motion (RIM), the Canadian corporation that provides those services, agrees to get "in line with UAE telecommunications regulations," by making unspecified accommodations to allow for government surveillance. The ban extends to BlackBerry devices used by foreigners [2], too. The UAE's Telecommunications Regulation Authority says [3] that "in their current form, certain BlackBerry services allow users to act without any legal accountability, causing judicial, social and national security concerns." RIM, in turn, has stated [4] that its Enterprise Server encryption is designed to ensure that no one, including RIM itself, can access a user's encrypted data. Reports indicate [5] that RIM has reached a tentative agreement with the Indian government over similar access concerns. Meanwhile, Saudi Arabia is following [6] in the UAE's footsteps.

The controversy raises a number of issues, including the question of what a company like RIM is supposed to do in order to be responsive both to its users and to local laws. We see at least three key issues:

1. Companies need to be more transparent about the deals they cut with governments. Let's be honest: All service providers cooperate with government surveillance to some degree, but unique concerns arise when the extent of cooperation is greater than publicly acknowledged. Users must be able to accurately assess the risks associated with the use of a particular communications tool.

2. Companies, advocates and policymakers need to resist the imposition of broad and ill-defined technological design mandates on communications services and products. Even the U.S. imposes certain requirements on certain service providers, but design mandates must be narrowly crafted, must recognize and protect the public value of secure communications, and, tying back to the first point, must be transparent.

3. Companies, advocates, and policymakers should insist on appropriate legal process for any governmental access. This should include particularized suspicion (no blanket surveillance) and independent judicial approval. And, in making deals with governments to gain market access, companies should be advancing user privacy rights and the rule of law as much as possible.

The recent stories focus on RIM's suite of mobile data services, such as email and BlackBerry Messenger. While all communications using these services apparently flow through RIM's Canadian data center, that is probably not the main issue, because all BlackBerry communications start by passing over the facilities of some local service provider, where they can be intercepted. Publicly, at least, there has been a lot of speculation about BlackBerry's encryption, but that may not be the bottom line issue either. BlackBerry services are available in a variety of configurations, and none of the reporting has been very clear about the differences. A major distinction is between "enterprise" services, which are used by corporations who issue BlackBerry devices to their employees, and consumer or individual services.

As far as we can tell, consumer or individual services are not encrypted by RIM technology. While RIM states in its public documentation [7] that all traffic between BlackBerry devices and Enterprise Servers is encrypted, it is talking just about its corporate services. Even corporate data is available in unencrypted form at the Enterprise Server. If the corporation runs its own Enterprise Server, and if the company is headquartered in the UAE, that server may be located within the UAE, and thus accessible to the government with the cooperation of the enterprise. However, if the Enterprise Server is located outside the UAE, the UAE might not have an easy way to compel the owner of the server to grant access to plaintext communications, and if the data is going from one enterprise user

to another, RIM would have no access to plaintext, even if the communications pass through its data center.

RIM's public statements also do not clarify the status of communications sent using services such as BlackBerry Messenger; even some messages from enterprise customers may also be available in unencrypted form from RIM.

Based on the press stories, it is hard to tell what the UAE and RIM are actually fighting about. What is clear is that there is a long-running, high-stakes negotiation between RIM and the UAE that likely involves different categories of information and different "access solutions" for different services and architectures. At the end of the day, RIM won't be able to satisfy all of the UAE's concerns – there are some configurations of the BlackBerry enterprise service that leave plaintext communications inaccessible to anyone except the system administrator for the enterprise. On the other hand, there are lots of unencrypted BlackBerry communications that will be available and lots of data associated with even encrypted communications that will be of value to the UAE police and security services. Moreover, the UAE may conclude that what is good for business – secure communications -- is good for the UAE, so it may quietly drop its demands for full access to everything. And certainly, the UAE's ability to host international business conferences or engage in multinational business transactions may decline if key business communications tools do not work there (or if corporate secrets are routinely exposed to the UAE government through some private deals between service providers and the UAE).

However, it does seem undeniable that RIM is cooperating with the UAE and other countries around the world to help those governments, to a greater or lesser degree, intercept and read the communications of BlackBerry users. Other service providers and equipment makers have likely done the same for their offerings.

Addressing Government Demands Worldwide

This brings us to one of our main points: the fact that it is so difficult to determine what is actually going on between RIM and the UAE and tough to figure out what is protected and what is not highlights the need for transparency about how RIM and other companies comply with government demands for design features and for assistance in carrying out surveillance. One doesn't want to give terrorists a blueprint for shielding their own communications, but the relationships between governments and service providers need to be more open. That is true not only in the UAE but also in Europe, the U.S. and the rest of the world.

It is hard for any one company to offer such transparency in isolation. Among other concerns, a company like BlackBerry is reluctant to publicize its dealings with one country for fear that it will immediately set a floor for demands by every other country. The fact that each deal is negotiated separately may keep governments off balance as well.

The only way we see to resolve this conundrum is by joint action: Companies, human rights advocates, and governments that care about privacy and Internet freedom must work together to define limits on government surveillance mandates, to bring greater transparency to such arrangements, and to set high standards for governmental access to communications.

Limiting Government Design Mandates

The UAE argues [8] that its regulators are only imposing on RIM the same obligations that the company faces under US law. The Emirati press release cites the US's Communications Assistance to Law Enforcement Act (CALEA), which requires telecommunications carriers to design their networks to ensure that there exists a technological means for law enforcement to intercept communications. This, it says, is identical to the set of demands that the UAE wants to impose upon RIM. In fact, CALEA, while flawed in some ways, is just the opposite of what we are seeing in the UAE and offers a much better approach to government demands.

First, CALEA is a public law, adopted by Congress after public hearings, and is implemented under the supervision of the Federal Communications Commission, whose decisions are in turn subject to

judicial review. It is unlikely that the UAE provides equivalent checks and balances on government design demands. Second, it is fairly clear that RIM is not covered by CALEA at all, because CALEA exempts "information services." Likewise, services used by corporations for their employees such as RIM's Enterprise Servers are not covered by CALEA, since CALEA does not apply to private networks.

Third, CALEA specifically recognizes the importance of unbreakable encryption to both commerce and human rights: CALEA includes a provision expressly stating that the Act gives the US government **no authority** to require a telecommunications carrier to design its encryption in such a way that the government can decrypt communications. Although the government may demand cryptography keys if the carrier chooses to retain them, it may not insist that they hold onto such keys in the first place. Fourth, the statute states that the standards adopted by industry for CALEA implementation must be public.

Rule of Law for Government Surveillance

Moreover, the debate highlighted by the BlackBerry dispute is not merely about design mandates. The other half of the equation is the government's authority to utilize those design features to intercept communications. In the US and most other democracies, in order to eavesdrop on a conversation or email or any other communication, law enforcement must obtain a court order, issued upon a finding of good cause and targeting a particular person. Even for national security purposes, targeting people in the U.S. requires a court order. We're no experts on UAE law, but we don't believe [9] that the Emirates have a truly independent judiciary or an equivalent, robust system of checks and balances.

Global Threat Needs Global Approach

RIM should not be left out there to resist government demands alone. It needs the concerted support of its competitors, of human rights advocates and of countries and international institutions that care about Internet freedom.

For the U.S., human rights advocacy must begin at home. After 9/11, the U.S. abandoned its strong commitment to privacy and due process, engaging in surveillance without court orders, making it possible for countries like the UAE and China to claim that their surveillance demands and practices were similar to those of the U.S. Earlier this year, Secretary of State Hillary Clinton promised that the US would once again become a leader for online privacy and free expression.

To lead, we have to get our own house in better order. One place to start would be restoring meaningful limits on some PATRIOT Act powers. Another would be to update the Electronic Communications Privacy Act. (Under ECPA, stored email is not fully protected. A major coalition [10] is urging reform of the law to raise the standard for access to stored email.) A third focus might be the Committee on Foreign Investment in the United States, which uses its broad authority to wring access concessions from communications service providers (possibly including RIM), and which discloses only statistical summaries of its work.

Globally, other democracies have also sought greater surveillance powers in recent years. The EU, for example, has adopted data retention mandates, requiring service providers to retain certain data for the convenience of the government. Policies that give short shrift to civil liberties place global technology companies in the difficult position of deciding which national laws to comply with and which laws to challenge.

Companies like RIM need support in determining how to draw principled lines when responding to governmental requests that could compromise the security of their products or increase the human rights risk to their users. One lesson we should draw from RIM's current challenge is that all companies should aggressively advocate for legal standards that respect human rights in all countries in which they operate, democratic and non-democratic alike. (The Global Network Initiative [11]strives to provide practical guidance for exactly these kinds of ethical dilemmas.) And in those countries without rule of law or democratically enacted public policy, companies must push back as much as possible against overreaching governmental requests that impact privacy of users,

and work to mitigate possible harm.

- UAE
- surveillance
- Free Expression
- blackberry

Links:
[1] http://[http://www.nytimes.com/2010/08/02/business/global/02berry.html
[2] http://[http://www.washingtonpost.com/wp-dyn/content/article/2010/08/02/AR2010080204752.html?wprss=rss_technology
[3] http://www.tra.ae/news_TRA_Announces_the_Suspension_of_Blackberry_Messenger%2C_Blackberry_E_mail_and_Blackberry_Web_Browsing_Services_in_the_UAE_from_October_11%2C_2010-180-1.php
[4] http://[http://www.arabianbusiness.com/594087-blackberrys-response-rim-statement-in-full
[5] http://economictimes.indiatimes.com/infotech/hardware/BlackBerry-to-open-code-for-security-check/articleshow/6249666.cms
[6] http://news.yahoo.com/s/afp/20100804/tc_afp/sauditelecomsecurityblackberry
[7] http://na.blackberry.com/eng/ataglance/security/features.jsp
[8] http://www.wam.org.ae/servlet/Satellite?c=WamLocEnews&cid=1278055857711&p=1135099400295&pagename=WAM%2FWamLocEnews%2FW-T-LEN-FullNews
[9] http://www.state.gov/g/drl/rls/hrrpt/2009/nea/136082.htm
[10] http://www.digitaldueprocess.org
[11] http://www.globalnetworkinitiative.org/