DRAFT 1/3/2006

Nine Options to Reduce Illegitimate Surveillance of the Internet

by

Lloyd S. Etheredge [1]

The discovery of widespread and illegitimate domestic and global surveillance of the Internet by the Bush Administration raises urgent issues for Internet architecture, governance, and public policy. Whatever the American government has done also will become a temptation for other governments and non-government (illicit) actors in the years ahead. It is timely to think boldly and creatively about political and engineering options to reduce illegitimate surveillance of Internet users, both individuals and corporations.

The following ideas are preliminary and intended for discussion, with the hope that their weaknesses will be more quickly identified. We can assume that any major government can, if it is a high priority, ultimately defeat any schemes to limit its surveillance - by new technology and/or by the more traditional methods of bribery, coercion, physical break-ins, or infiltration. However the security against illegitimate surveillance of most Internet users can be increased by deploying a range of options that increase the difficulties, costs and risks of engaging in such unwanted activities.

[1] This is a draft and comments are welcome: lloyd.etheredge@yale.edu and (301)-365-5241. Lloyd Etheredge is Director of the Government Learning Project at the Policy Sciences Center in New Haven, CT.

I. Political Options

1.) Remove the President's Power to Classify Information about Domestic Surveillance Without Court Supervision

Currently, in America, it is a serious federal crime to disclose classified material. These laws should remain, but Congress also should amend the Patriot Act to remove the President's power to classify domestic surveillance that is undertaken by the Executive branch, without a court warrant, after the first fifteen days of a national emergency or declaration of war.[2] This change makes it more likely that whistle blowers will quietly inform the press and Congress of any questionable activity and permit the American system of checks and balances to operate.

2.) Redirect Surveillance to Chosen International Targets, and Use Public Disclosure for Deterrence

It may be possible to achieve political agreement to focus NSA's Internet surveillance on countries that are not democracies and that sponsor international terrorism. Any country on the State Department's watch list could be placed on public notice and subjected to aggressive (secret) communication surveillance, including taps on all forms of communications entering or leaving the country (Internet, wireline and wireless telephone, mail, electronic financial transac-

[2] At the moment (January 2006) it is worth noting that all three branches of the US government have failed to provide democratic checks on the Bush Administration's illegitimate NSA surveillance initiatives. And that only one newspaper (The New York Times) has been willing to break the story - and it delayed more than a year. Concerning lesson-drawing for historical experience and the curtailment of secrecy laws, see Daniel P. Moynihan, Secrecy: The American Experience (New Haven: Yale University Press, 1999). I am indebted to Lynn Etheredge for discussion of this option and other comments.

tions) as well as monitoring of international travelers and 24x7 high definition satellite surveillance of suspicious activity. The efforts to intercept international traffic by wholesale monitoring of the Internet backbones that cross North America and other advanced industrial countries would end; physical surveillance of Internet and other communications would be placed near the borders of the target countries.

It has been widely reported that sophisticated terrorists already know that their cell phones (for example) are being tapped. But being explicit about the range and capacities for American electronic (and other) surveillance could be a deterrent. It would sober people about the amount of work that is required for secrecy, and the costs and risks of attempting to incite violence beyond their borders.

3.) Professional Counter-Surveillance

We are likely to discover that Internet-related companies are sometimes pressured to cooperate illegitimately with governments - for example, to program the Internet's routing computers to send copies of all Internet messages to a government agency or permit clandestine physical taps of their fiber optic backbones. One solution is to develop an Internet Security Inspection Service with a multinational membership, similar to the IAEA (International Atomic Energy Agency), empowered to receive tips and complaints and conduct snap inspections of routing computers and other physical facilities in all nations and offer whistle-blower compensations to informants who suffer professional harm for disclosing illegitimate behavior. The service could be run by an existing intergovernmental organization like the ITU (International Telecommunications Union) or trusted private entities. The Internet Security Inspection Service could, at a minimum, warn the public of adverse findings or of non-cooperation and their findings could influence decisions concerning contracts for the operation of the Internet backbones and Internet architecture.[3] An agreement to cooperate with the Internet Security Inspection Service could become a legal requirement for all companies that operate Internet backbones.

II. Coding Options for all Internet Traffic

Today, encryption and decryption of email can be done automatically by computers, using many methods. If we think about the illegitimate surveillance that has already occurred, it is probably a worthwhile investment (and deterrent to future trouble) to make strong encryption of all Internet traffic a standard (default) option. Simple add-in modules for browsers or email programs can provide a range of options, and the encryption or decryption can operate in the background.[4] To cite three methods:

4.) Number-Based, One-Time-Use Codes

It is widely agreed that one-time-use codes are, if they meet other requirements, virtually

[3] An Internet Security Inspection Service is not simply an anti-US step. It could bring to light a great many compromises of Internet security, by a range of non-US government and non-government actors.

[4] There are many techniques that can be incorporated into browsers and email programs. See David Kahn, The Codebreakers: A Comprehensive History of Secret Communication from Ancient Times to the Internet (NY: Scribner, 1996). Revised and updated edition.

unbreakable. Thus, several public Internet security sites could Webcast streams of time marks and random digits (or prime numbers, selected at random) for encryption. A simple software program would allow any pair of users to select a series of time marks and record the associated numbers, with the sequence of time marks and code-creating numbers changing for each message. (Thus, the time mark need not be the time that the message is sent: a time mark could be at 12:06 AM and 10.53 seconds GMT seven months ago.) Over the years, the paired software programs could store as many code numbers as required - and, of greater significance, the many trillions of digits and time marks transmitted by the Internet security sites, across the years, could overwhelm reasonable systems of physical storage and retrieval by an intelligence service with illegitimate motives, even if it later discovered the time marks agreed upon. If mathematically desirable, it would be straightforward to increase the number of Internet security sites (to 1,000?) and their rates to millions of bits/second.

5.) Text-Based, One-Time-Use Codes

A classic spycraft method is to use numbers that refer to literary texts so that even number-crunching supercomputers can be thwarted. [For example, a seven-digit number could be created to refer to the page number (up to three digits), line number (up to two digits) and sequential position of a word from the left margin (up to two digits) in a selected edition of the Bible.] Now that millions of volumes are about to become available online it would be straightforward to write software that allows a pair of users to select a unique sequence of volumes (or a random sequence of volumes) in online libraries that are “known” only to the encoding and decoding disks they initially create. [5]

6.) Photography-Based One-Time Use Codes

A third technical option is to use hidden messages while fooling outside observers about the existence of a hidden message. A simple software program could provide each pair of users with identical disks containing a series of digital photographs. The sender's computer program alters, in a way invisible to the naked eye, minor details of selected pixels to encode a message, with the changes being automatically detected by the recipient's computer program that has the original photograph for reference.[6] The accompanying message simply reads; "Here is young Charles on his sixth birthday. Miss you - ." Picture-encoding technology could be an ideal method for sending coded email messages from cell phones, which can store and send a series of stored pictures.

- Each of these methods also can be adapted by leading Internet portals, search services, and Websites. Google, for example, could offer choices of software encryption packages to its customers, and receive disks from each user with their choice of individualized, one-time-use

[5] Traditionally, one of the practical limitations of the system was that it required each spy in a foreign country to own, or have access to, a physical copy of the book. Today, when millions of books in many languages can be viewed online, and are downloadable, the method becomes more attractive.

[6] The same techniques could be applied to selections of music, including subtle (digital) changes at frequencies that cannot be detected by the human ear. Or to pre-recorded voicemail messages ("Sorry to have missed you. Just calling to wish you a Happy New Year!")

encryption schemes for a sequence of visits. (From that point, the processes of encryption and decryption would be automatic and invisible, at both ends.) The IT Departments of large organizations (universities, corporations) could routinely handle such issues for individual users so that, for example, all Google searches by students and the faculty will be (routinely and automatically) private and protected by strong (one-time-use) encryption firewalls.

III. Internet-Architecture Techniques

Two further challenges can be addressed by upgrades in Internet architecture and protocols: a.) Making it very difficult for an outsider to intercept most of the parts of any message; b.) Disguising the sending and/or receiving addresses for Internet traffic. Again, no option is perfect, but the cost to defeat them can be a deterrent to all but the most committed and well-financed intruder. Here are three ideas:

7.) Multi-Route, Maximum Dispersal Options

Currently, Internet packets are routed automatically, by specialized computers, to maximize efficiency. But the Internet has abundant spare capacity - less than 2% of existing fiber optic strands are lit - and a part of this spare capacity can be used for security. It would be straightforward to change Internet protocols to allow user-designated routing that (for example) avoided any Internet backbone crossing the North American continent. Or the packets of a message could be sent by twenty different international geographical routes, across lines owned and operated by different companies. Or twenty different routes designated at random. The expense to monitor many Internet backbones and branches could be increased exponentially.

8.) Multi-Device, Multi-Route Options

It would be relatively easy to divide any email message into packets transmitted by different technologies and companies with different originating and intermediate addresses (that then forward their subset of packets to a final destination). For example, a user could supply his computer with a list of the communication devices and email accounts that he owns. In turn, the computer would divide the packets of any (encoded) outgoing message among them: a.) transmit some packets via the Internet from each of several email accounts; b.) transmit some packets via cell phone email to a cut-out account (registered in the name of another user) for forwarding; c.) use a dial-up modem to call a Skype number in another country and transmit some packets via its network. To defeat the technique, a great many computers would have to monitor many different circuits of communications, operated by different companies, in many different countries, and do an enormous amount of processing, just to recover a message that could be encrypted with an almost unbreakable one-time-use method.

9.) Swiss-Based Email Addresses and Spoofing Sites.

Another option depends upon locating at least one highly trustworthy country with well-enforced and strong legal protections for personal and corporate confidentiality. To provide security to its users, any Website could create a mirror site in Switzerland. And a Swiss Internet Service Provider might register 500 billion separate Internet addresses in Switzerland (*.ch) and assign one of them as a “spoof” address to any pair of users who wish confidentiality for Website searching or email.

Thus: anybody who wishes their Google searches to be confidential would address encrypted (one-time-code) search requests from their home computer to a unique “spoof” address in Switzerland, which would forward the request to the Swiss mirror site of Google. Google’s Swiss site would automatically decrypt the request, run the search, and encrypt the reply for retransmission from the “spoof” address.[7] The American NSA could observe that a huge volume of the world’s Internet traffic increasingly moved across Swiss borders but they could not identify who was talking to whom or visiting which Website. And probably could not decipher the content.

[7] Yahoo or Google (or a Swiss contractor who runs a secure mirror site for them) could arrange the one-time-use codes (see option 6, above) for users who wish to have the option.