Serve Yourself: Shifting Power Away from the Brothers

Ian Brown[1] and Gus Hosein[2]

This piece with links is available online at: http://www.cs.ucl.ac.uk/staff/I.Brown/little-brother/

1. Big Brother is going distributed. Why should Big Brother do all the work, with an (Inter)network of Little Brothers to hand? CALEA'd telcos and banks who "know their customer" are just two examples of intermediaries co-opted through government regulation to store reams of information on their customers. Little Brothers have all the advantages of other distributed systems - scalability, reliability, high performance... We need to take decentralisation one step further, and claw back control from Big Brother and his little siblings.

2. Big Brother loves Client/Server Computing. Limited bandwidth and processing power in personal computers has led many systems to offload work and data to centralised systems. But as customer computing resources have increased, we have not taken back processing to the privacy-friendly enviroment of our own PCs. Governments have always co-opted intermediaries as little brothers: banks with "know your customer" and other "money laundering" regulations; airlines performing passenger identification for "safety" and immigration requirements; and telcos with wiretapping laws for "national security". If intermediaries are built, They will come.

3. New infrastructure brings new institutions. The new Internet economy is thus still only partly decentralised. New intermediaries like Amazon hold even more information with efficient identification and searching mechanisms, leaving more information in far wider industries open to similar government coercion—data waiting to be matched. As thick and strong as walls can be built around these decentralised data resources, none are impervious to the familiar knock on the door, with or without subpeona, warrant, or regulation. E-mail, viewing preferences, purchases, payment mechanisms, transaction records—all linked together by the perfect key: your identity. Big Brother is laughing all the way to the (data) banks.

4. Why not alter the environment? We are stuck with partially-decentralised systems. The only privacy solution in this environment of intermediaries is anonymised or pseudonymised records. We should use the newly available processing power and bandwidth to create full disintermediation. Ask the questions: Why were governments excited by Certification Authorities? For an old idea—key escrow. Why have CAs instead of personal key certification? Extend this: Why deliver e-mail through centralised servers? Why anonymise through proxies rather than clients? Why virtual network through a provider and not directly to the other computer? Why Application Service Providers? Why service providers at all? The processing resources exist, the bandwidth resources exist, the protocol resources are developing... so serve yourself. The knock will then have to be on your door, because the information will not exist elsewhere.

5. Then let the new economy replicate this new infrastructure. Disintermediate banks the way the Postal Service was disintermediated by e-mail: create personal fund manager schemes where users store e-cash locally, lending it out in a global on-line capital market, and spending anonymously through a smartcard or over encrypted Internet links. Don't rely on one telco for your communications and security requirements—use end-to-end encryption and location privacy across several networks. Vested interests will fight hard to prevent this change, but technology has circumvented these interests before, and can do so again.
6. The pipes exist... let's do some plumbing. Don't call the plumber, serve yourself.

Decentralised e-mail delivery

E-mail is a great example of how very small design changes can greatly affect the privacy of a system.

The vast majority of current mail clients deliver your messages first to your own mail server, which forwards them to your recipient's mail server, where they remain until collected.[3] This was appropriate 20 years ago when Internet connectivity was relatively patchy, and mail servers would deliver messages in batches when a link was available. But today's core network is available 24/7. Why shouldn't your message be delivered directly to your recipient's mail server? This prevents it passing through your ISP's mail server, whose administrator may store copies of outgoing messages, scan mail for "interesting" information, or undertake myriad other privacy-unfriendly practices. Even better, as more and more users gain permanent Internet connections through cable modems or Digital Subscriber Lines, why not bypass their mail server too and deliver direct to their PC?

This becomes doubly important with the [Direct, secure mail links] ability of Netscape Communicator and other mailers to deliver mail over secure Transport Layer Security links[4] (as used for secure Web browsing). Setting up a secure link to your local mail server is of little use if your messages can be intercepted there or on the remaining insecure path to your recipient. While end-to-end message encryption with PGP or S/MIME is slightly safer, secure delivery provides a transparent alternative for users who have not set up such software[5].

Hands off!

Any centrally-stored information can be abused. Whether it is the trawling of 80,00 files on a Singaporean business service by government authorities[6], the court-ordered release of anonymous subscriber identities by Yahoo[7], or personal characteristics tricked from AOL by the US Navy[8], information wants to be free. Authorities and institutions want to benefit from this new availability and are usually ably assisted by intermediaries.

Governments are working to 'update' their laws and regulations to authorise their own access to information such as ISP logs and e-mail. The UK government is rushing through the appropriately acronymed Regulation of Investigatory Powers Bill[9], which will set requirements for tapping facilities for ISPs and start the ball rolling on 'Codes of Practices' allowing police unwarranted access.

This is the continuation of closed meetings held in 1998 between the Association of Chief Police Officers and the Internet Service Providers Association that created a forum to "develop an accepted procedure for requesting and providing information."[10] The suggested procedure attempted to sidestep data protection legislation and did not require a warrant. But British interception warrants are signed and authorised by politicians anyway.

These approaches represent a time gone by. Instead of placing our faith in institutions determined to "maintain the status quo,"[11] we must question our models. If you store information anywhere but your own computer, expect it to be released upon request. If you send any information unencrypted, assume it will be intercepted.

Rather than rely on institutions and laws to protect privacy, we must keep information out of their jurisdictional reach.

Footnotes

[1] Department of Computer Science, University College London, Gower Street, London WC1E 6BT, UK. http://www.cs.ucl.ac.uk/staff/I.Brown/

[2] Tutorial Fellow, Department of Information Systems, London School of Economics and Political Science, Houghton Street, London WC2A 2AE, UK. http://is.lse.ac.uk/staff/hosein/

[3] Jon Postel. Simple Mail Transfer Protocol. RFC 821, August 1982. http://sunsite.auc.dk/RFC/rfc/rfc821.html

[4] Tim Dierks and Chris Allen. The TLS Protocol. RFC 2246, November 1997. http://sunsite.auc.dk/RFC/rfc/rfc2246.html

[5] Adam Back and Ian Brown. Reducing vulnerability to private key compromise. Working paper, March 1998. http://www.cs.ucl.ac.uk/staff/I.Brown/pfs2.html

[6] Peng Hwa Ang and Berlinda Nadarajan. Censorship and the Internet: A Singaporean Perspective. Communications of the ACM, Vol.39, No.6, June 1996. http://www.acm.org/pubs/citations/journals/cacm/1996-39-6/p72-ang/

[7] Courtney Macavinta. Yahoo message board suit continues. CNET News.com, March 1, 1999. http://news.cnet.com/news/0-1005-200-339276.html

[8] Janet Kornblum. Navy, AOL settle privacy case. CNET News.com, June 12, 1998. http://news.cnet.com/news/0-1005-200-330209.html

[9] Foundation for Information Policy Research. Interception of Communications Information Centre. http://www.fipr.org/ioca/

[10] Tim Pearson. A response from ISPA and ACPO/ISP/Government Forum to Cyber-Rights and Cyber-liberties UK, December 2, 1998. http://www.cyber-rights.org/privacy/response.htm

[11] Janet Reno. Law Enforcement In Cyberspace. Presented to The Commonwealth Club Of California, San Francisco, California, June 14, 1996. http://www.cs.georgetown.edu/~denning/Reno-Commonwealth.txt