

**SAN FRANCISCO NEIGHBORHOOD
ANTENNA-FREE UNION**
1835 Broderick Street
San Francisco, CA 94115
(415) 885-1981
www.antennafreeunion.org

September 28, 2005

Mayor Gavin Newsom
City Hall, Room 200
1 Carlton B. Goodlett Place
San Francisco, CA 94102

TechConnect RFI/C 2005-07
Dept. of Telecommunications & Information
Services
875 Stevenson Street, 5th Floor
San Francisco, CA 94103

Re: **San Francisco TechConnect WiFi Broadband Initiative**

Dear Mayor Newsom:

I am writing on behalf of the San Francisco Neighborhood Antenna-Free Union (SNAFU), a grass-roots, city-wide coalition of community organizations and individual residents, to express strong, unequivocal opposition to your San Francisco TechConnect wireless fidelity ("WiFi") broadband initiative based on two primary grounds: (1) the potential health and environmental risks posed by the radiation used by WiFi networks; and (2) the difficulty and cost of adequately securing such networks, which if done cheaply and improperly poses the risk of identity theft, loss of personal privacy, and the unauthorized monitoring of individuals who use such a network. This letter will also serve as SNAFU's official response to the Department of Telecommunications and Information Services' Request for Information (RFI) on this proposal.

Background

As you are acutely aware from your years as a Supervisor, thousands -- perhaps tens of thousands -- of San Francisco residents are deeply concerned about the potential health impacts of proliferating wireless technologies in their communities. Since 2001, no fewer than 15 Conditional Use Appeals concerning cellular phone base station antennae have been brought before the Board of Supervisors. In 12 of those cases, the Board has granted residents' appeals and denied the permit sought by the wireless carrier involved. While the Board has been preempted by federal law from considering residents' health concerns in these appeals and residents have therefore prevailed on other issues, health considerations have clearly been a principal concern among those who have brought these appeals, and continue to be so.

Unlike these appeals heard by the Board of Supervisors, your proposed WiFi broadband initiative is not subject to federal preemption of consideration of health and environmental issues, for two primary reasons: (1) WiFi operates in an area of the electromagnetic spectrum currently unlicensed by the FCC and not subject to the Telecommunications Act of 1996; and (2) it is the City and County of San Francisco itself (perhaps in contractual agreement with one or more wireless providers), and not a licensed wireless carrier, that is considering providing WiFi to City residents. The City's duty to protect the health, safety and welfare of its citizens, including protection from the potential health and environmental impacts of pervasive, low-level modulated microwave radiation, as well as its recent adoption of the Precautionary Principle, virtually mandate that such considerations be taken into account.

Health & Environmental Effects of Radio Frequency Radiation (RFR)

WiFi networks, like their digital cellular phone counterparts, utilize low-level, modulated radio frequency radiation (RFR) in the microwave range to transmit their signals. As Dr. Henry Lai of the University of Washington, one of the world's leading experts on the biological effects of RFR, stated at San Francisco State University in March 2005, in the past 30-35 years there have been somewhere between 2,000 to 3,000 scientific studies done on the biological effects of RFR. According to Dr. Lai, of these studies only approximately 230 have specifically involved cellular phones and their antennae, given the relatively recent widespread adoption of this technology on a global scale. Of these, in excess of 70% of the studies funded independently of the cellular phone industry identify biological effects of RFR at the low power levels typical of cell phones and cellular base station antennae. (Attached as Exhibit A is a selective list compiled by Dr. Lai of RFR studies and their reported biological effects. See *Updated List of Studies Finding Biological Effects at Low Intensities of RF Radiation Provided by Henry Lai, Ph.D., "Information & Research," www.protectschools.org.*)

The United States Environmental Protection Agency (EPA) itself acknowledges that current Federal Communications Commission (FCC) radiation protection standards are inadequate and do not account for all possible harmful effects of RFR, in particular the non-thermal effects that are of particular relevance to the radiation utilized by the WiFi network you are proposing. In a July 16, 2002 letter from Norbert Hankin of the EPA's Center for Science and Risk Assessment, Radiation Protection Division to Janet Newton, President of The EMR Network, Mr. Hankin writes: "The FCC's current exposure guidelines, as well as those of the Institute of Electrical and Electronics Engineers (IEEE) and the International Commission on Non-Ionizing Radiation Protection, are thermally based, and ***do not apply to chronic, nonthermal exposure situations.***" (Emphasis added.) (Attached as Exhibit B is a copy of Hankin's letter. See *EPA Letter Outlining the Need for More Protective Standards for Radiofrequency (RF) Radiation, "Information & Research," www.protectschools.org.*)

Additionally, the United Kingdom has recently officially recognized a condition known as electrosensitivity as a legitimate and increasingly prevalent public health problem. (Attached as Exhibit C is an article from *The Sunday Times – Britain*, dated 9/11/05.) In this respect, the U.K. follows Sweden, which similarly declared electrosensitivity an officially recognized disability in 2000. While the United States government has yet to officially recognize electrosensitivity and the City and County of San Francisco is under no legal obligation to do so, in light of these recent developments in Great Britain it arguably has a moral obligation to consider the effects its policies may have on those so afflicted.

Finally, the City's Department of Telecommunications and Information Services (DTIS) has been aware from at least March 2003 of residents' health concerns about WiFi, but has incorporated none of these concerns in its San Francisco TechConnect proposal. (Attached as Exhibit D is a copy of minutes of DTIS's March 31, 2003 hearing, including my testimony on behalf of SNAFU regarding this issue.) This runs directly counter to the City's Precautionary Principle ordinance, which states that "the community has a right to know complete and accurate information on potential human health and environmental impacts associated with the selection of products, services, operations or plans. ***The burden to supply this information lies with the proponent, not with the general public,***" and that "an obligation exists to examine a full range of alternatives and select the alternative with the least potential impact on human health and the environment including the alternative of doing nothing" (Emphasis added.)

If as Mayor you are truly interested in making San Francisco a model 'green' city, there should be no place in this model for a potentially injurious technology like WiFi.

Inherent Insecurity of Wireless Networks

If the potential health risks presented by wireless technology is one area manufacturers and vendors of this technology wish to keep under wraps, another is the inherent insecurity of wireless networks. WiFi is particularly vulnerable to hacking, including identity theft and theft of confidential information, due to flaws in software (e.g., the ubiquitousness of Windows software with all of its known and steadily-continuing-to-be-revealed security flaws and corresponding patches); flaws in hardware (e.g., the Linksys WRT54G, a "consumer" wireless networking product that received *PC Magazine's* "Editors' Choice" award in June 2005, is now three months later the subject of an article entitled "Serious' security holes in Linksys [Cisco] router" in *SearchSecurity*, September 14, 2005); and the serious limitations of commonly used security practices (such as encryption, authentication, etc.). As Kelly Martin writes in "Catching a Virus Writer," (www.securityfocus.com/columnists/246, attached as Exhibit E):

Mayor Gavin Newsom
TechConnect RFI/C 2005-07
September 28, 2005
Page 4

With the consumer WiFi explosion, launching a virus into the wild has never been easier and more anonymous than it is today. . . . Even a robustly secured wireless access point can be cracked in a matter of hours. The extreme, industrial-strength security afforded using LDAP and/or RADIUS and rotating keys ciphers is possible, but not for the faint of heart. In other words, for tens of thousands of access points across the country and around the globe, basic wireless security is already irrelevant. For someone searching for a novel launch point for their virus, your router might just be the next in line.

In addition, a truly robust security protocol will likely not easily accommodate many different users with differently configured and outfitted computers who want to quickly and easily access the Internet via WiFi hotspots in the kind of model you envision for San Francisco. This level of inconvenience is not going to be acceptable to users who want to log in at any coffee shop or bus stop and quickly do whatever they want to do over the Internet. Moreover, how does the City plan to administer such a robustly secured network? Given how easy, anonymous and financially rewarding hacking and Internet theft have become, how many security personnel are you prepared to pay for to ensure that your TechConnect network does not become a magnet for every industrious criminal enterprise across the country or around the world? In short, to truly secure a wireless network is an extremely expensive and complex task, and it is highly unlikely that a municipal government like ours will be willing to spend what it takes.

In closing, I doubt that you wish your legacy as Mayor to include that of a mindless purveyor of cheap techno-junk who was prepared to jump on the nearest bandwagon at the expense of your residents' security and well-being. As residents of San Francisco, we deserve better than this.

Sincerely,



Doug Loranger

12/27/04

Studies reporting biological effects of radiofrequency radiation (RFR) at low intensities

- (1) Balode (1996)- blood cells from cows from a farm close and in front of a radar showed significantly higher level of severe genetic damage.**
 - (2) Boscol et al. (2001)- RFR from radio transmission stations (0.005 mW/cm²) affects immunological system in women.**
 - (3) Chiang et al. (1989)- people lived and worked near radio antennae and radar installations showed deficits in psychological and short-term memory tests.**
 - (4) de Pomerai et al. (2000, 2002) reported an increase in a molecular stress response in cells after exposure to a RFR at a SAR of 0.001 W/kg. This stress response is a basic biological process that is present in almost all animals - including humans.**
 - (5) de Pomerai et al. (2003) RFR damages proteins at 0.015-0.020 W/kg.**
 - (6) D'Inzeo et al. (1988)- very low intensity RFR (0.002 – 0.004 mW/cm²) affects the operation of acetylcholine-related ion-channels in cells. These channels play important roles in physiological and behavioral functions.**
 - (7) Dolk et al. (1997)- a significant increase in adult leukemias was found in residence who lived near the Sutton Coldfield television (TV) and frequency modulation (FM) radio transmitter in England.**
 - (8) Dutta et al. (1989) reported an increase in calcium efflux in cells after exposure to RFR at 0.005 W/kg. Calcium is an important component of normal cellular functions.**
 - (9) Fesenko et al. (1999) reported a change in immunological functions in mice after exposure to RFR at a power density of 0.001 mW/cm².**
 - (10) Hjollund et al. (1997)- sperm counts of Danish military personnel, who operated mobile ground-to-air missile units that use several RFR emitting radar systems (maximal mean exposure 0.01 mW/cm²), were significantly low compared to references.**
 - (11) Hocking et al. (1996)- an association was found between increased childhood leukemia incidence and mortality and proximity to TV towers.**
 - (12) Ivaschuk et al. (1999)- short-term exposure to cellular phone RFR of very low SAR (26 mW/kg) affected a gene related to cancer.**
-

(13) Kolodynski and Kolodynska (1996)- school Children lived in front of a radio station had less developed memory and attention, their reaction time was slower, and their neuromuscular apparatus endurance was decreased.

(14) Kwee et al. (2001)- 20 minutes of cell phone RFR exposure at 0.0021 W/kg increased stress protein in human cells.

(15) Lebedeva et al. (2000)- brain wave activation was observed in human subjects exposed to cellular phone RFR at 0.06 mW/cm².

(16) Magras and Xenos (1999) reported a decrease in reproductive function in mice exposed to RFR at power densities of 0.000168 - 0.001053 mW/cm².

(17) Mann et al. (1998)- a transient increase in blood cortisol was observed in human subjects exposed to cellular phone RFR at 0.02 mW/cm². Cortisol is a hormone involved in stress reaction.

(18) Marinelli et al. (2004)- exposure to 900-MHz RFR at 0.0035 W/kg affected cell's self-defense responses.

(19) Michelozzi et al. (1998)- leukemia mortality within 3.5 km (5,863 inhabitants) near a high power radio-transmitter in a peripheral area of Rome was higher than expected.

(20) Michelozzi et al. (2002)- childhood leukemia higher at a distance up to 6 km from a radio station.

(21) Navakatikian and Tomashevskaya (1994)- RFR at low intensities (0.01 - 0.1 mW/cm²; 0.0027- 0.027 W/kg) induced behavioral and endocrine changes in rats. Decreases in blood concentrations of testosterone and insulin were reported.

(22) Novoselova et al. (1999)-low intensity RFR (0.001 mW/cm²) affects functions of the immune system.

(23) Park et al. (2004) higher mortality rates for all cancers and leukemia in some age groups in the area near the AM radio broadcasting towers.

(24) Persson et al. (1997) reported an increase in the permeability of the blood-brain barrier in mice exposed to RFR at 0.0004 - 0.008 W/kg. The blood-brain barrier envelops the brain and protects it from toxic substances.

(25) Phillips et al. (1998) reported DNA damage in cells exposed to RFR at SAR of 0.0024 - 0.024 W/kg.

- (26) Polonga-Moraru et al. (2002) change in membrane of cells in the retina (eye) after exposure to RFR at $15 \mu\text{W}/\text{cm}^2$.
- (27) Pyrpassopoulou et al. (2004) exposure to cell phone radiation during early gestation at SAR of $0.0005 \text{ W}/\text{kg}$ ($5 \mu\text{W}/\text{cm}^2$) affected kidney development in rats.
- (28) Salford et al. (2003)- nerve cell damage in brain of rats exposed for 2 hrs to GSM signal at $0.02 \text{ W}/\text{kg}$.
- (29) Santini et al. (2002)- increase in complaint frequencies for tiredness, headache, sleep disturbance, discomfort, irritability, depression, loss of memory, dizziness, libido decrease, in people who lived within 300 m of mobile phone base stations.
- (30) Sarimov et al. (2004)- GSM microwaves affect human lymphocyte chromatin similar to stress response at $0.0054 \text{ W}/\text{kg}$.
- (31) Schwartz et al. (1990)- calcium movement in the heart affected by RFR at SAR of $0.00015 \text{ W}/\text{kg}$. Calcium is important in muscle contraction. Changes in calcium can affect heart functions.
- (32) Somosy et al. (1991)- RFR at $0.024 \text{ W}/\text{kg}$ caused molecular and structural changes in cells of mouse embryos.
- (33) Stagg et al. (1997)- glioma cells exposed to cellular phone RFR at $0.0059 \text{ W}/\text{kg}$ showed significant increases in thymidine incorporation, which may be an indication of an increase in cell division.
- (34) Stark et al. (1997)- a two- to seven-fold increase of salivary melatonin concentration was observed in dairy cattle exposed to RFR from a radio transmitter antenna.
- (35) Tattersall et al. (2001)- low-intensity RFR ($0.0016 - 0.0044 \text{ W}/\text{kg}$) can modulate the function of a part of the brain called the hippocampus, in the absence of gross thermal effects. The changes in excitability may be consistent with reported behavioral effects of RFR, since the hippocampus is involved in learning and memory.
- (36) Vangelova et al. (2002)- operators of satellite station exposed to low dose ($0.1127 \text{ J}/\text{kg}$) of RFR over a 24-hr shift showed an increased excretion of stress hormones.
- (37) Velizarov et al. (1999) showed a decrease in cell proliferation (division) after exposure to RFR of $0.000021 - 0.0021 \text{ W}/\text{kg}$.
-

(38) Veyret et al. (1991)- low intensity RFR at SAR of 0.015 W/kg affects functions of the immune system.

(39) Wolke et al. (1996)- RFR at 0.001W/kg affects calcium concentration in heart muscle cells of guinea pigs.

Source of literature and abstracts:

(1) Balode, Z, Assessment of radio-frequency electromagnetic radiation by the micronucleus test in bovine peripheral erythrocytes. *Sci Total Environ* 180(1):81-85, 1996.

Previous bioindicative studies in the Skruna Radio Location Station area have focused on the somatic influence of electromagnetic radiation on plants, but it is also important to study genetic effects. We have chosen cows as test animals for cytogenetical evaluation because they live in the same general exposure area as humans, are confined to specific locations and are chronically exposed to radiation. Blood samples were obtained from female Latvian Brown cows from a farm close to and in front of the Skruna Radar and from cows in a control area. A simplified alternative to the Schiff method of DNA staining for identification of micronuclei in peripheral erythrocytes was applied. Microscopically, micronuclei in peripheral blood erythrocytes were round in shape and exhibited a strong red colour. They are easily detectable as the only coloured bodies in the uncoloured erythrocytes. From each individual animal 2000 erythrocytes were examined at a magnification of x 1000 for the presence of micronuclei. The counting of micronuclei in peripheral erythrocytes gave low average incidences, 0.6 per 1000 in the exposed group and 0.1 per 1000 in the control, but statistically significant ($P < 0.01$) differences were found in the frequency distribution between the control and exposed groups.

(2) Boscol P, Di Sciascio MB, D'Ostillo S, Del Signore A, Reale M, Conti P, Bavazzano P, Paganelli R, Di Gioacchino M. Effects of electromagnetic fields produced by radiotelevision broadcasting stations on the immune system of women. *Sci Total Environ* 273(1-3):1-10, 2001.

The object of this study was to investigate the immune system of 19 women with a mean age of 35 years, for at least 2 years (mean = 13 years) exposed to electromagnetic fields (ELMFs) induced by radiotelevision broadcasting stations in their residential area. In September 1999, the ELMFs (with range 500 KHz-3 GHz) in the balconies of the homes of the women were (mean +/- S.D.) 4.3 +/- 1.4 V/m. Forty-seven women of similar age, smoking habits and atopy composed the control group, with a nearby resident ELMF exposure of < 1.8 V/m. Blood lead and urinary trans-trans muconic acid (a metabolite of benzene), markers of exposure to urban traffic, were higher in the control women. The ELMF exposed group showed a statistically significant reduction of blood NK CD16+ CD56+, cytotoxic CD3(-)-CD8+, B and NK activated CD3(-)-HLA-DR+ and CD3(-)-CD25+ lymphocytes. 'In vitro' production of IL-2 and interferon-gamma (INF-gamma) by peripheral



UNITED STATES ENVIRONMENTAL PROTECTION AGENCY
WASHINGTON, D.C. 20460

JUL 16 2002

OFFICE OF
AIR AND RADIATION

Ms. Janet Newton
President
The EMR Network
P.O. Box 221
Marshfield, VT 05658

Dear Ms. Newton:

This is in reply to your letter of January 31, 2002, to the Environmental Protection Agency (EPA) Administrator Whitman, in which you express your concerns about the adequacy of the Federal Communications Commission's (FCC) radiofrequency (RF) radiation exposure guidelines and nonthermal effects of radiofrequency radiation. Another issue that you raise in your letter is the FCC's claim that EPA shares responsibility for recommending RF radiation protection guidelines to the FCC. I hope that my reply will clarify EPA's position with regard to these concerns. I believe that it is correct to say that there is uncertainty about whether or not current guidelines adequately treat nonthermal, prolonged exposures (exposures that may continue on an intermittent basis for many years). The explanation that follows is basically a summary of statements that have been made in other EPA documents and correspondence.

The guidelines currently used by the FCC were adopted by the FCC in 1996. The guidelines were recommended by EPA, with certain reservations, in a letter to Thomas P. Stanley, Chief Engineer, Office of Engineering and Technology, Federal Communications Commission, November 9, 1993, in response to the FCC's request for comments on their Notice of Proposed Rulemaking (NPRM), Guidelines for Evaluating the Environmental Effects of Radiofrequency Radiation (enclosed).

The FCC's current exposure guidelines, as well as those of the Institute of Electrical and Electronics Engineers (IEEE) and the International Commission on Non-ionizing Radiation Protection, are thermally based, and do not apply to chronic, nonthermal exposure situations. They are believed to protect against injury that may be caused by acute exposures that result in tissue heating or electric shock and burn. The hazard level (for frequencies generally at or greater than 3 MHz) is based on a specific absorption dose-rate, SAR, associated with an effect

that results from an increase in body temperature. The FCC's exposure guideline is considered protective of effects arising from a thermal mechanism but not from all possible mechanisms. Therefore, the generalization by many that the guidelines protect human beings from harm by any or all mechanisms is not justified.

These guidelines are based on findings of an adverse effect level of 4 watts per kilogram (W/kg) body weight. This SAR was observed in laboratory research involving acute exposures that elevated the body temperature of animals, including nonhuman primates. The exposure guidelines did not consider information that addresses nonthermal, prolonged exposures, i.e., from research showing effects with implications for possible adversity in situations involving chronic/prolonged, low-level (nonthermal) exposures. Relatively few chronic, low-level exposure studies of laboratory animals and epidemiological studies of human populations have been reported and the majority of these studies do not show obvious adverse health effects. However, there are reports that suggest that potentially adverse health effects, such as cancer, may occur. Since EPA's comments were submitted to the FCC in 1993, the number of studies reporting effects associated with both acute and chronic low-level exposure to RF radiation has increased.

While there is general, although not unanimous, agreement that the database on low-level, long-term exposures is not sufficient to provide a basis for standards development, some contemporary guidelines state explicitly that their adverse-effect level is based on an increase in body temperature and do not claim that the exposure limits protect against both thermal and nonthermal effects. The FCC does not claim that their exposure guidelines provide protection for exposures to which the 4 W/kg SAR basis does not apply, i.e., exposures below the 4 W/kg threshold level that are chronic/prolonged and nonthermal. However, exposures that comply with the FCC's guidelines generally have been represented as "safe" by many of the RF system operators and service providers who must comply with them, even though there is uncertainty about possible risk from nonthermal, intermittent exposures that may continue for years.

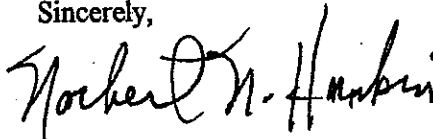
The 4 W/kg SAR, a whole-body average, time-average dose-rate, is used to derive dose-rate and exposure limits for situations involving RF radiation exposure of a person's entire body from a relatively remote radiating source. Most people's greatest exposures result from the use of personal communications devices that expose the head. In summary, the current exposure guidelines used by the FCC are based on the effects resulting from whole-body heating, not exposure of and effect on critical organs including the brain and the eyes. In addition, the maximum permitted local SAR limit of 1.6 W/kg for critical organs of the body is related directly to the permitted whole body average SAR (0.08 W/kg), with no explanation given other than to limit heating.

I also have enclosed a letter written in June of 1999 to Mr. Richard Tell, Chair, IEEE SCC28 (SC4) Risk Assessment Work Group, in which the members of the Radiofrequency Interagency Work Group (RFIAWG) identified certain issues that they had determined needed to be addressed in order to provide a strong and credible rationale to support RF exposure guidelines.

Federal health and safety agencies have not yet developed policies concerning possible risk from long-term, nonthermal exposures. When developing exposure standards for other physical agents such as toxic substances, health risk uncertainties, with emphasis given to sensitive populations, are often considered. Incorporating information on exposure scenarios involving repeated short duration/nonthermal exposures that may continue over very long periods of time (years), with an exposed population that includes children, the elderly, and people with various debilitating physical and medical conditions, could be beneficial in delineating appropriate protective exposure guidelines.

I appreciate the opportunity to be of service and trust that the information provided is helpful. If you have further questions, my phone number is (202) 564-9235 and e-mail address is hankin.norbert@epa.gov.

Sincerely,



Norbert Hankin
Center for Science and Risk Assessment
Radiation Protection Division

Enclosures:

- 1) letter to Thomas P. Stanley, Chief Engineer, Office of Engineering and Technology, Federal Communications Commission, November 9, 1993, in response to the FCC's request for comments on their Notice of Proposed Rulemaking (NPRM), Guidelines for Evaluating the Environmental Effects of Radiofrequency Radiation
- 2) June 1999 letter to Mr. Richard Tell, Chair, IEEE SCC28 (SC4) Risk Assessment Work Group from the Radiofrequency Radiation Interagency Work Group

www.timesonline.co.uk
TIMES ONLINE
 The best of The Times and The Sunday Times, in real time

ENTER **The World Challenge**

- ARCHIVE CLASSIFIED SHOPPING PROMOTIONS GAMES FAST TIMES MY TIMES

Search

September 16 2005

MAKE TIMES ONLINE
 YOUR HOMEPAGE / BOOKMARK

SUNDAY TIMES
TIMES ONLINE

- Home
- Britain
- World
- Business
- Money
- Sport
- Comment
- Travel
- Entertainment
- Tech & Net
- Law
- Crossword
- Driving
- Property & Gardens
- Women
- Health
- Jobs
- Food & Drink
- Books
- Education
- Student
- Sunday Times
- Site Map

SPECIAL REPORTS

- Making Skills Work
- European Cities
- Arts Power 100
- The Art of Travel
- Child Welfare
- At Your Service
- Snapshot of summer
- Men's Style
- Everyday Revolution
- French Film Café

The Sunday Times - Britain

September 11, 2005

Electrical fields can make you sick

SARAH-KATE TEMPLETON, MEDICAL CORRESPONDENT

A GOVERNMENT agency has acknowledged for the first time that people can suffer nausea, headaches and muscle pains when exposed to electromagnetic fields from mobile phones, electricity pylons and computer screens.

The condition known as electrosensitivity, a heightened reaction to electrical energy, will be recognised as a physical impairment.

A report by the Health Protection Agency (HPA), to be published next month, will state that increasing numbers of British people are suffering from the syndrome. While the total figure is not known, thousands are believed to be affected to some extent.

The report, by the agency's radiation protection division, is expected to say that GPs do not know how to treat sufferers and that more research is needed to find cures. It will give a full list of the symptoms, which can include dizziness, irregular heartbeat and loss of memory.

Although most European countries do not recognise the condition, Britain will follow Sweden where electrosensitivity was recognised as a physical impairment in 2000. About 300,000 Swedish men and women are sufferers.

The acknowledgement may fuel legal action by sufferers who claim mobile phone masts have made them ill.

In January Sir William Stewart, chairman of the HPA and the government's adviser on mobile phones, warned that a small proportion of the population could be harmed by exposure to electromagnetic fields, and called for careful examination of the problem.

The HPA has now reviewed all scientific literature on electrosensitivity and concluded that it is a real syndrome. The condition had previously been dismissed as psychological.

The findings should lead to better treatment for sufferers. In Sweden people who are allergic to electrical energy receive government support to reduce exposure in their homes and workplaces.

CLASSIFIEDS

- TRAVEL
- CARS
- JOBS
- ENCOUNTERS
- PROPERTY

GO

Choice of the week

GO

SERVICES

- ARCHIVE
- E-MAIL BULLETINS
- FAST TIMES
- CROSSWORD CLUB
- FANTASY GAMES
- COMPETITIONS
- SHOPPING
- WEATHER

GO

ADVERTISING



Business Travel

SEARCH TIMES ONLINE

TRAVEL

JOBS

- **Holidays**
- **Marketplace**
- **Insurance**
- **Check -In**
- **Travel bulletin**
- **New brochures**
- **Holiday partners**

RSS NEWS FEEDS FROM **TIMES ONLINE**

NEWSPAPER EDITION

- ▶ **THE TIMES**
- ▶ **THE SUNDAY TIMES**

epaper

THE TIMES AND THE SUNDAY TIMES ELECTRONIC PAPER

Special cables are installed in sufferers' homes while electric cookers are replaced with gas stoves. Walls, roofs, floors and windows can be covered with a thin aluminium foil to keep out the electromagnetic field — the area of energy that occurs round any electrically conductive item.

British campaigners believe electrical devices in the home and the workplace, as well as mobile phones emitting microwave radiation, have created an environmental trigger for the syndrome.

There is particular concern about exposure to emissions from mobile phone masts or base stations, often located near schools or hospitals.

In January Stewart also called for a national review of planning rules for masts. The review was launched by the government in April.

British sufferers report feeling they are being "zapped" by electromagnetic fields from appliances and go out of their way to avoid them.

Some have moved to remote areas where electromagnetic pollution is lower.

The HPA report is eagerly awaited by campaigners. Alasdair Phillips, director of the campaign group Powerwatch, said: "This will help the increasing number of people who tell us their GPs do not know how to treat them."

Rod Read, chairman of Electrosensitivity UK, added: "This will be the beginning of an awareness of a new form of pollution from electrical energy."



ALSO IN THIS SECTION

- Doctors in 'cash for visas' scam
- Ditch Holocaust day, advisers urge Blair
- Bush bungled Katrina crisis, say Britons
- Union leaders tell Blair to quit within the year
- New pub law will fuel rape and murder, say police

Ads by Google

British Gas price freeze
British Gas offers frozen energy prices until 2010
www.house.co.uk

Suffer From Bloating?
See what products work well in well in dealing with Bloating.
www.ConsumerHealthDigest.com

Natural Digestive Enzyme
Highest Grade Digestive Enzyme Stop Bloat After Meals. Guaranteed
www.proflpamy.com

electricity
Get the cheapest electricity online
Fantastic deals. Visit now!
www.CheapSeek.co.uk

- LATEST**
- Free bet**
Visit Sp
betting
- Travel**
Search
ideas for
- Film Fil**
For free
preview
- Depart**
Your on
- Outdoc**
25% sa
readers
- Resear**
Browse
reviews
- Jobs**
Search
our wee
- Studen**
For a co
- Busine:**
Search
compan
- Busine:**
Find the
the SME

Contact our advertising team for advertising and sponsorship in Times Online, The Times and The Sunday Times.

Copyright 2005 Times Newspapers Ltd.

This service is provided on Times Newspapers' standard Terms and Conditions. Please read our Privacy Policy .
To inquire about a licence to reproduce material from The Times, visit the Syndication website.



Telecommunications Commission

March 31, 2003, Special

SPECIAL MEETING OF THE
TELECOMMUNICATIONS COMMISSION
CITY AND COUNTY OF SAN FRANCISCO

MINUTES

March 31, 2003

CITY HALL
ROOM 400

5:30 P.M.

COMMISSIONERS

Kim Bogen, President
J. Michael Myatt, Vice President
Sunil V. Daluvoy
Elizabeth Inadomi
Michael Rouan

Helen Danina, Commission Secretary
Lewis Loeven III, Executive Director
DEPARTMENT OF TELECOMMUNICATIONS
AND INFORMATION SERVICES (DTIS)

1. CALL TO ORDER AND ROLL CALL

The meeting was called to order by Acting Chair Myatt at 5:30 p.m., and roll was called by the Commission Secretary.

Present: Vice President J. Michael Myatt

Commissioner Sunil V. Daluvoy

Commissioner Elizabeth Inadomi

Commissioner Michael Rouan

Absent: President Kim Bogen

2. APPROVAL OF THE MINUTES OF February 24, 2003

Acting Chair Myatt requested to abstain from voting on the February 24, 2003 minutes, because he was not present. Commissioner Inadomi made a motion, seconded by Commissioner Daluvoy, to exempt Acting Chair Myatt from voting on the

adoption of the February 24, 2003 minutes. The Commission moved to grant Acting Chair Myatt an abstention with three ayes [Daluvoy, Inadomi, Rouan]; none opposed.

Public Testimony: none.

Commissioner Rouan made a motion, seconded by Commissioner Inadomi, to approve the minutes of February 24, 2003. The Commission moved to adopt the minutes with three ayes [Daluvoy, Inadomi, Rouan] and one abstention [Myatt]; none opposed.

3. COMMUNICATIONS

The descriptions of the communications received by the Commission are listed at the end of the agenda.

Public Testimony - none.

Commissioner Comments - none

3. DIRECTOR'S REPORT

Emergency Communications Department (ECD)

Executive Director praised the teamwork demonstrated by the staff at the Department of Telecommunications and Information Services (DTIS) and the ECD during the anti-war protests this month. Four extra channels were made available in response to the 50% increase in calls at ECD, and to ensure that the City's 800MHz system gave public safety providers adequate service.

Both the DTIS and the ECD technicians made the Computer Aided Dispatch system operate efficiently despite the increased activity. Executive Director Loeven thanked Executive Director Sullivan of ECD and the DTIS and ECD technicians, and commented that the call answer times were reduced even though call activity increased.

Budget

DTIS staff is working with various City departments to ensure that the telecommunications and IT services are not compromised by budget deficits during the next fiscal year. The Department is working with the SFGTV to increase access to public meetings by acquiring equipment that will allow public meetings to be carried on the government cable channel without increasing staff. The City's web site has increased collection of City revenues by 27% over the past year, through payments for parking tickets, business taxes and other City services.

CA Channel

Comcast has moved the California Channel programming off the public access channel. That move limits the freeing up of the public access channel to subscribers on the digital system that is approximately 40% of the City. Brian Wilson and Brian Roberts of DTIS met with Mr. Blaney to clarify the SFCTC's concerns and to plan for making the public access channel available 24/7 to all San Francisco subscribers.

Comcast Rebuild

DTIS staff will review Comcast's rebuild progress report, delivered on March 31, 2003, to determine current progress, to make projections for the next six months, and to

consider options.

Executive Director Loeven thanked Ms. Linda Crayton and Comcast for seeking to resolve this issue quickly. He also thanked SBC for helping DTIS with switching equipment.

Public testimony: none.

Commissioner comments: none.

5. DEPUTY DIRECTOR'S POLICY REPORT

Deputy Director Brady highlighted the following topics:

File 021884 (Public Access Cable Television)

- At the March 25 meeting, the Board of Supervisors approved a resolution designating San Francisco Community Television Corporation (SFCTC) as responsible for the management and operation of the public access channel (Access San Francisco) through June 30, 2005.
- The resolution approved the public access grant awarded to SFCTC by DTIS and the Telecommunications Commission on October 28, 2002.

FCC seeks comments on "do-not-call" law

- The FCC released a notice of proposed rulemaking on March 25, 2003, seeking comment on rules regarding unwanted telephone solicitations consistent with FTC "do-not-call" lists.
- The Do-Not-Call Implementation Act signed this month requires the FCC to report to Congress within 45 days after it has completed its rules, and to report annually after that.

The following persons spoke during public testimony:

Kazmi Torii, member of the Producers and Programmers Network of San Francisco, asked for clarification regarding the extension of the SFCTC's grant. Deputy Director Brady replied that the department must ask the Board of Supervisors to extend the grant designation during the stated time period, June 30, 2005.

Karl Bryant, Treasurer, Producers and Programmers Network of San Francisco, asked whether the Commission would allow the Producers and Programmers Network of San Francisco to continue to contest the award of any contract to SFCTC unless they were involved in the granting of the award.

Commissioner comments: none

6. NEW BUSINESS

Telecommunications Plan Update

- Status of consumer broadband (cable/DSL/satellite) availability in San Francisco

Brian Roberts, DTIS, Senior Policy Analyst gave the following presentation:

- The Plan was adopted in January 2001, and must be updated every two years, as required by the Administrative Code (Sec. 11.88(f));
- This presentation focuses on residential broadband, which was identified in the original Plan. Competition was expected in the downtown business district, but less in residential areas. The Plan also identified the financial concerns of the telecommunications industry, and what the retrenchment of investment has had in residential broadband;
- Although the Plan was issued in 2001, it relied on a survey of telecommunications companies made in 1998, on telephone and mail surveys done in 1999, and on periodic Commission hearings.
- There were three facilities-based carriers: SBC, Comcast, and RCN.
- Some partially facilities-based carriers were examined by the Plan, including competitive local exchange carriers (CLECs) such as Northpoint and Covad.
- Fixed wireless/satellite were mentioned in the Plan because they were emerging at time Plan was issued.
- The Commission wanted consumers to have a choice of advanced, affordable telecommunications services. The policies of the Commission intended to facilitate entry, open access, support for low income discounts, and support for public access.
- Comcast covers 40% of the City and anticipates covering an additional 86,000 houses within the next six months, and RCN covers 9% of the City. The only independent Data CLECs that remains is Covad. Sprint Direct has withdrawn and Direcway is marketing in rural areas.
- Broadband distribution is high in San Francisco; 40% of the online population has high-speed data (38% DSL, 2% cable modem).
- There has been a tendency to bundle the high speed data with other services. There have been different prices for different speeds.
- Data CLECs is highly subject to regulation. The FCC recently decided that in order to get low cost access to the home, they have to share part of the frequency on a copper line with the Telephone Company.
- Wi-fi was not contemplated in the original Plan. Wi-fi was mostly considered a "wireless LAN" product for the home or office.
- Broadband alternatives and competition in the marketplace

Center for Digital Democracy

- Gary Larson represents the Center for Digital Democracy, a non-profit organization based in Washington, D.C., which monitors telecommunications policy to ensure that the digital media systems serve the public interest by preserving openness and diversity of the Internet.

- Larson is encouraged by the Telecommunications Plan of San Francisco because it promotes the democratic process of telecommunications services to the residents and businesses of San Francisco.
- He said the biggest challenge is preparation of an informed and demanding citizenry.
- Non-commercial, educational, public interest programming is concerned with devoting some franchise fees to PEG programming.
- Portland is looking at wi-fi networks associated with their existing infrastructure. Some cities are expanding their I-Nets beyond their schools, libraries, and public buildings to community centers and cultural organizations.
- San Francisco could create virtual real estate for the arts community.
- Besides commercial uses, some of the new services should be devoted to non-commercial, public interest programming.

SBC

Byron McDaniel, SBC Vice President of Construction and Engineering, discussed the following topics in the attached presentation:

- Network overview;
- Services overview;
- Map of DSL service in San Francisco;
- Future of SBC - Mission Bay
- Architecture of fiber;
- Summary

Comcast

Linda Crayton, Director of Government Affairs at Comcast introduced the Comcast representatives: John Aragon, Vice President of Government Affairs; Brent Bayon, Director of Engineering; Amy Lurch, Director of Sales and Market; Heather Tawes, Manager of Marketing; Tom Tantriella, Manager of Network Construction. The presentations given at the meeting and attached hereto included:

- Linda Crayton regarding Comcast in California:
- Tom Tantriella regarding completed districts of the upgrades of San Francisco homes passed, Comcast infrastructure, rebuild impediments in San Francisco.
- Amy Lynch regarding the new broadband services in San Francisco, and customer services in the Bay Area.

Cisco

Eric Blaufarb, Cisco Systems Field Marketing Manager, Wireless Networking Business Unit, gave a PowerPoint presentation (attached) as an overview of wireless technology applications for first responders to provide wireless LAN coverage at local libraries, universities, hotels, and airports.

Intel

Kevin Kahn, Intel Fellow, in a PowerPoint presentation (attached) stated that wi-fi is inexpensive and works as a short-range innovative technology to provide public coverage in "hotspots" such as airports, cafes, parks, universities. Wi-fi technology will become essential in public transit waiting rooms. Police departments use wi-fi. Other areas of the world are ahead of the U.S. in wi-fi deployment.

The following persons spoke during public testimony:

Jack Fuchs, Vice President of SOMA Networks, San Francisco, <http://www.somanetworks.com/>, spoke about last-mile broadband that can be deployed quickly and inexpensively to the underserved community, and to provide choices to other communities. Wireless technology is available for the last mile. He suggested that equipment be installed on the base of existing cell sites to provide broadband, data, and voice services. He indicated that consumers can be connected to the internet by plugging a small device into a computer and standard telephone line. Wide area technology is the solution for the last hundred feet into the home.

Duncan Davidson explained that Skypilot, brings broadband services to incumbent ISPs through open access mesh networking, which overcomes distance. If the network architecture is correct, and more people can join, more capacity, greater coverage, and increased speed are achieved. The network topology improves with density. He encouraged the Commission to investigate the new technologies, particularly open spectrum wi-fi unlicensed systems.

Steve Zeltzer, Vice Chair of Producers and Programmers Network of San Francisco, asked why many San Franciscans have no access to new technologies like broadband, while in South Korea, for example, 70% of the population has access. He contends that Comcast charges high rates, forces acquisition of digital, and is not user friendly. Further, Comcast censors anti-war ads, and is anti-unions. He favors wi-fi and democratic communications.

Zeltzer stated that the Community Television Corporation (CTC) has less live programming in community access now than it did when it was under TCI. Finally, the programmers have been told by CTC that they must become members in order to participate at CTC. He believes this to be undemocratic, and urges that the City control the new technologies, as in Ashland, Oregon, where the cable and internet system is owned by the City. To learn about democratic communications, he recommended the one-day seminar, "Access, Broadband and the Digital Future" scheduled on April 5, 2003 at Stanford University.

Doug Loranger represented the San Francisco Neighborhood Antenna-Free Union (SNAFU), a city-wide coalition of local residents and neighborhood organizations that focuses on the impacts of wireless technologies in San Francisco. He said that the City is revising the 1996 Wireless Telecommunications Services Facilities Siting Guidelines. The Planning Commission on March 13, 2003 voted to hold a joint hearing between the Planning Commission and the Board of Supervisors Land Use Committee to consider legislation drafted by Supervisor Ammiano to revise these guidelines. He distributed to the Commissioners a one-hour documentary that focuses on siting wireless facilities and the concerns of San Francisco residents.

Loranger asked that the public health impact of the rapidly evolving wireless technologies be a part of any discussion taking place by City agencies with respect to these technologies. He was disturbed that the wireless presentation held at the regular meeting of the Telecommunications Commission of February 24, 2003 did not include such a discussion. He reminded the Commission that the City's Telecommunications Master Plan and the Telecommunications Commission itself came into existence because of residents' concerns about the health effects of the first and second generations of wireless technology in San Francisco.

Mark Longwood cited studies (attached) by a number of physicians on the health effect of electromagnetic fields.

Pamela Gaddies, a producer at Channel 29, stated that she is concerned about the health of the African American community in San Francisco. She noted that none of the technology addresses the health disparity among the African Americans.

Todd Curtis addressed the Commission regarding the health concerns surrounding wireless cell sites. He stated that residents of the Mission District are appealing a decision by the Planning Commission to issue conditional use permits for antennae.

As a new RCN customer, he is concerned that RCN does not provide public access cable. He understood that RCN cable service in San Francisco must provide public access channels.

Commissioner Inadomi asked for clarification from Brian Roberts, Linda Crayton, and Byron McDaniel regarding broadband policies or practices in San Francisco, including any associated with wi-fi. Byron McDaniel replied that currently there is no product associated with wi-fi and the company is evaluating whether they want a SBC product or a partner product. Comcast replied that they do not distribute the product.

Commissioner Daluvoy asked Comcast and SBC what is the timeframe between homes passed and services provided, and about SBC's fiber-based network. Commissioner Daluvoy then questioned Intel and SkyPilot regarding security and interference.

Commissioner Rouan stated that there was a need to examine the health issues. RCN will provide PEG for public access. He expressed support for video-on-demand and streaming opportunities for PEG.

7. CALENDAR MATTERS

The regular meeting of the Telecommunications Commission will occur on April 28, 2003 at City Hall, Room 400, 5:30 p.m.

Public testimony: none.

Commissioner comments: none

Review of Telecommunications Commission Pending Topics List.

Public testimony: none.

Commission comments: none.

6. GENERAL PUBLIC TESTIMONY

Kazmi Torii, member of the Producers and Programmers Network of San Francisco, asked about the mandatory membership requirement instituted at CTC. Also, she thought that non-profit status would improve public access, and wondered why there is a budget shortfall at CTC.

8. ADJOURNMENT

Acting Chair Myatt adjourned the meeting at 8:00 p.m.

Respectfully submitted,

Helen C. Danina

Catching a Virus Writer

Kelly Martin,

With the consumer WiFi explosion, launching a virus into the wild has never been easier and more anonymous than it is today.

Like a sneeze in a crowded subway, it's hard to find the human source of the latest viral infection. On the Internet it's not much different. The people who write these nasty little programs and release them into the wild almost never get caught. Why? The answer is easy, but it's also a sort of technical nemesis: there's simply no way to track these people down.

The current approach to catching virus writers isn't working. Code analysis and disassembly provides clues about the author, but it's not enough. Virus writers boast of their accomplishments in private bulletin boards, yet only the most vocal and arrogant few will get caught. Even with logs, IP addresses and private access, it's still near impossible to track them down.

Law enforcement agencies in every country are clearly ill-equipped to deal with the myriad of technical hurdles required to track virus authors down, and so they turn to a few elite security consultants, some working as threat analysts at the major A/V vendors for help. They can usually narrow down the source of a virus to having been released in a geographic part of the world, but the rest is a mere packet in the bitstream.

Add Microsoft's new \$250,000 bounty into the mix and at first glance, you'd think we're right on track. Not a chance! There are simply too many ways to be anonymous on the Internet, and more so today than ever before. You don't even need to spoof IP addresses these days; there are too many ways to have perfect stealth. Imagine you're a virus writer and need a launchpad for your evil work. Just start with an untraceable MAC address on a borrowed IP address, linked into a wireless router down the street which has access logging disabled, and then you tunnel through countless proxies and compromised zombies until you reach the desired launch point. Someone who does not wish to be caught (and knows what they're doing), cannot be caught. With wireless, it becomes a physical battle between a million victims and one guy walking down the street.

Why WiFi?

WiFi has exploded. Welcome to the truly anonymous Internet. There is no easier way to slip on and off the Internet now without being noticed than on an insecure 802.11x wireless network in a coffee shop, under a tree in Central Park, at a library or even just leaked through the walls of the apartment next door. North America, and indeed the rest of the world, already has an incredible number of wireless devices that are effectively free, unsecured, and readily available to anyone -- to such an extent that it's more difficult to **avoid** these sprawling networks than it is to connect to them now. My Mac with embedded g-band happily connects to just about any network it can find, and it appears there are literally dozens, perhaps hundreds of insecure wireless Access Points now within a short walking distance from my office.

There are a mind-boggling number of WiFi devices now, and only the ubiquity of these

devices is new: while four or five years ago I may have been the first on my block with WiFi, now there are so many devices I have to worry about interference to make sure I'm using the right pipe.

More than that, there are a mind-boggling number of wireless access point that are not Secure by Default, out of the box -- just like the machine owned by your average Microsoft Windows user. But even if they were, it wouldn't matter.

I live in a sparsely-populated area, at least for a major metropolitan city. Yet without even leaving the couch of my living room, I can "borrow" someone else's Internet connection, mask my MAC address and have complete stealth on the Internet. It would be difficult, if not impossible, to ever track me down or prove a request or download came from me.

If I wanted to be a bit smarter about things, however, I'd walk to the park and get my access from there... less likely that the police come knocking on my door. Or I'd drive down to the coffee shop, and setup a launch from there. Or better still: point my homemade antenna (made out of a soup and used according to the exacting laws of wavelengths and physics) and bounce the signal off a digital satellite dish, extending my network's range by up to 2km. In other words, I could literally get my Internet access from home by simply pointing my directional antenna towards metropolitan downtown.

I have no malicious intent, however. I'm generally not searching for these insecure networks, they just appear all on their own. When I'm not publishing articles on SecurityFocus, I go for coffee at a shop at the bottom of our building. There is free wireless Internet access available, sure -- though I'm not sure if it's actually provided by the coffee shop, or if it's coming from an office next door, or below me, or above me -- the service has never been advertised. The owner of the shop doesn't know what wireless access means. One day I was sitting down and drinking chai... I opened up my Mac with OS X, and there was a new network(broadcasting itself, with no security). Most Windows machines, by default, similarly connect to the strongest local signal without discretion, and voila.

I check the connection, and can instantly surf the web. SSH works fine, and thus secure (and dynamic) SSH tunnels are possible. And secure email, through port 993, is possible as well. Web access, like usual, is in the clear (except when using SSL and then it too, is secure). No security whatsoever. It's wide open. I drink my chai and imagine opening up a can of worms... or rather, imagine someone logging onto his bot network through IRC, sitting anonymously in some coffees shop, drinking espresso and launching DDoS (distributed denial-of-service) attacks.

If I fudge my MAC address and make up a fake one, it will be impossible for anyone to know it's me. I'll change the apparent MAC address again tomorrow and maybe I'll sit in a different coffee shop, too.

Free but insecure networks

What I'm trying to get at is this "promiscuity" of wireless networks has already made security on the Internet redundant -- a virus writer using this technology could never be tracked down. There are hundreds of access points within a five kilometer radius of me, and the number is growing every day. Having had 802.11x access myself for a long time, I clearly know that the technology and its weaknesses are hardly new. What's new is the proliferation of access points, the vast majority of which are freely available for personal use.

Even a robustly secured wireless access point can be cracked in a matter of hours. The extreme, industrial-strength security afforded using LDAP and/or RADIUS and rotating keys ciphers is possible, but not for the faint of heart. In other words, for tens of thousands of access points across the country and around the globe, basic wireless security is already irrelevant. For someone searching for a novel launch point for their virus, your router might just be the next in line.

Salon published an interesting (and entertaining) article by Micah Joel (requires free day pass) about the opening up access points and its legal implications: no security, broadcast the SSID, and turn logging off. Encourage people, in fact, to use the free connection. With no way to know who has used your Internet connection, there's no way that you could be held liable for inappropriate (or illegal) use. You'd be just like everyone else who took it out of the box, and plugged it in. No officer, you can't possibly prove that action was taken by me. While this theory has yet to be help up in court, at least here in Canada, a precedent is waiting to be set. It's already being done almost everywhere. Don't believe me? CNN published an article recently only confirming what many of us already knew: the insecurity of wireless networks has become extreme.

Of course, it would be just as easy to launch a virus from an Internet café in many other parts of the world, like Asia and India where anonymous access is given for a mere dollar an hour. And then there are the libraries, colleges, user groups and other institutions everywhere else that, once again, provide a bastion of easy, cheap anonymity.

Let me now be clear about my motivations: while I do not have the skills to write a virus myself, there are many, many people out there who do. Writing it and sharing code is one thing; launching it into the wild is another thing altogether. Similarly, technical stealth is now very easy to achieve in a multitude of ways, so we're left to rely on the social components to catch a writer writer: a coder who shows some arrogance, perhaps does some public code sharing, things that will ultimately do him in. The only way he might be caught is if one of his inner-circle friends squeal on them -- and then traditional law enforcement steps in, grabs all the electronic equipment, and the forensics start. You might think the informant has a good chance at getting that juicy \$250,000 bounty, but once he's linked to that inner circle of people sharing code, the token bounty once again fades into the mist.

Virus writers can launch their dubious malcode from just about anywhere in the world, a form of cyber-terrorism that cannot be stopped. Anonymity is generally a good thing, but not always. The promiscuity of the Internet is here.

Privacy Statement
Copyright 2005, SecurityFocus