ROBERT GELLMAN
Privacy and Information Policy Consultant **202-543-7923**
419 Fifth Street SE **bob@bobgellman.com**
Washington, DC 20003

Trafficking in Health Information: A Widespread Problem

By Robert Gellman

Version 1.6
April 16, 2007

http://bobgellman.com/rg-docs/rg-health-traffic.pdf

Surreptitious trafficking in health information may be common and nationwide. This conclusion is based on evidence collected by the House Committee on Government Operations in 1979 and in 1994. The following discussion is based partly on the Committee's 1994 legislative report accompanying a legislative proposal to enact a federal Fair Health Information Practices Act.[1] Much of what follows is a direct quote from that report, but some additional material has been added from an earlier congressional report[2] and from other sources. An update from a 2006 United Kingdom report strongly suggests that the same activities are universal and ongoing.

The Denver Investigation

The best-documented American example of abuse of health records comes from Denver, Colorado. Beginning in 1975, the Denver District Attorney and a grand jury began an investigation of the theft of health records. They found that for over twenty-five years, a private investigative reporting company known as Factual Services Bureau, Inc., engaged in a nationwide business of obtaining health information without the consent of the patient. **Factual Services Bureau advertised that it would obtain medical information about claimants who did not provide a medical authorization or who submitted partial information to the insurance company.**

The customers of Factual Services Bureau included over one hundred of the most prominent insurance companies in the country. In a search of the Denver office of Factual Services Bureau, the District Attorney found almost two thousand reports to insurance companies. These reports frequently included detailed medical information about individuals that was obtained without the knowledge or consent of the individuals. No insurance company ever reported this questionable activity to law enforcement authorities.

The company's investigators typically posed as doctors and sought medical information by telephone from public and private hospitals, clinics, and doctors' offices,

[1] House Committee on Government Operations, Health Security Act, H.R. Rep. No 103-601 Part 5 (1994). The proposal did not become law.
[2] House Committee on Government Operations, Federal Privacy of Medical Information Act, H.R. Rep. No. 96-832 Part 1 (1980).

including psychiatrists' offices. The company paid hospital employees to smuggle out health records. Another technique involved the use of false pretenses through mail solicitations. The company was successful in obtaining health records most of the time, and it even advertised its ability to acquire health records.

In June 1976, the Denver grand jury issued a special report to the Privacy Protection Study Commission. The report stated that trafficking in patient records was a nationwide problem:

> **From the evidence, it is clear that the problem with respect to the privacy of medical records in this jurisdiction exists in many cities and jurisdictions across the nation.**[3]

In testimony submitted to the Committee during 1979 hearings, Denver District Attorney Dale Tooley said:

> I find it difficult to believe that there are not or have not been similar enterprises engaged in this profitable, surreptitious business.[4]

Other U.S. Evidence

Additional direct evidence that this type of trafficking in health information is widespread in this country is hard to find because there have been no investigations focusing on health records in recent years. However, evidence of trafficking in other types of personal information is easy to find. For example, the General Accounting Office reported on misuse of criminal history information maintained by the National Crime Information Center (NCIC).[5] GAO found that the NCIC system was vulnerable to misuse, that misuse occurred throughout the NCIC system, and that some misuse was intentional, including using the system for personal purposes, such as looking up friends, relatives, or neighbors. A limited review by GAO found sixty-two examples involving misuse, including these two:

> The California Department of Justice received a complaint from a person who suspected his employer of obtaining a copy of his criminal record from the NCIC's [Interstate Identification Index] file. A search of the state system's audit trail showed that the record had been accessed by a law enforcement agency in the eastern United States. Apparently, the employer had hired a private investigator, located in the eastern United States, to conduct background searches on prospective employees. The complainant's criminal history record was allegedly sold to the private investigator by an officer in a law enforcement agency.[6]

> A private investigator paid several city employees to conduct NCIC record searches. During the service of a search warrant at the investigator's office in an

---

[3] Privacy Protection Study Commission, *Personal Privacy in an Information Society* at 285 (1977).
[4] *Privacy of Medical Records*, Hearings before a Subcomm. of the House Comm. on Government Operations, 96th Cong., 1st Sess. 1066 (1979).
[5] General Accounting Office, *National Crime Information Center: Legislation Needed to Deter Misuse of Criminal Justice Information* (GAO/T-GGD-93-41) (1993).
[6] Id. at 24.

> unrelated fraud matter, state investigators discovered records indicating that payments had been made for NCIC records and notified the Colorado Bureau of Investigation. The ensuing inquiry, with the cooperation of the district attorney, resulted in the indictment of several individuals.[7]

These examples are similar to the illegal buying and selling of personal information uncovered by the Denver grand jury.

Other types of sensitive personal records are also routinely bought and sold. One investigation found a nationwide network of information brokers who obtained information from the NCIC, the National Law Enforcement Telecommunications System, the Military Personnel Records Center, the Social Security Administration, the telephone companies, and others. The information was provided in exchange for money by insiders who knew that it was against the law and policy of their agency or company.[8] There is even evidence of open solicitation through newspaper advertising of the ability to obtain records that are legally protected against improper disclosure.[9]

Health Record Traffcking in Canada

Evidence supporting the notion that there is routine illegal trafficking in health information also comes from Canada. In 1979, Mr. Justice Horace Krever, Commissioner of the Royal Commission of Inquiry into the Confidentiality of Health Records in Ontario, Canada, testified before the Subcommittee on Government Information and Individual Rights.[10] The Royal Commission of Inquiry had its origins in press stories about abuse of confidential health information. Mr. Justice Krever testified that at the time the inquiry began, no one had any clear idea of the extent of the violation of confidentiality, or that many violations were in the private casualty insurance sector.[11]

The Royal Commission found that the acquisition of health information by private investigators without patient consent and through false pretenses was widespread. During a 14-month period, the Royal Commission heard from over 500 witnesses, including private investigative firms, insurance companies, hospitals, and others. For the years 1976 and 1977, the Royal Commission found that there were hundreds of attempts made in Ontario to acquire health information from hospitals and doctors; well over half of the attempts were successful. Several investigative firms went out of business as a result of the Royal Commission's work.[12]

The way in which the Royal Commission found these abuses is illustrative of the difficulties of conducting an investigation in this area. The role of investigative agencies and

---

[7] Id. at 26.
[8] See *Sale of Criminal History Records*, Hearing before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary, 102d Cong., 2d Sess. 7 (1992) (Serial No. 87) (testimony of David F. Nemecek, Federal Bureau of Investigation).
[9] Id.
[10] *Privacy of Medical Records*, Hearings before a Subcomm. of the House Comm. on Government Operations, 96th Cong., 1st Sess. 499-553 (1979).
[11] Id. at 508.
[12] Id. at 508-536.

insurance companies came to light primarily as a result of the suspicions of a nurse in a small hospital near Niagara Falls. One night, the nurse received a phone call from someone claiming to be employed in a Toronto emergency room. The caller said that information about a patient – who had previously been treated at the Niagara Falls hospital – was needed for emergency treatment.

The nurse was suspicious and said that she would return the call. However, when she checked the phone number, she found that it did not belong to the Toronto hospital that the caller named. Several additional calls for information were made, but the nurse refused to release any data.

Because the nurse had written down and kept the phone number, she was later able to give it to the Royal Commission staff. Based on this lead, the staff was able to trace the phone number to a specific investigative firm and gather enough evidence to apply for a search warrant of the firm's offices. The search produced files disclosing that medical information was obtained through false pretenses on a wholesale basis. The firm even hired registered nurses to make the pretext phone calls.

Using this information, the Royal Commission obtained search warrants for insurance companies that used the services of the investigative firm. This in turn led the Commission to other private investigative firms that had similar operations and then to other insurance companies. **In this manner, the entire practice, which had not even been suspected at first, was exposed.** Mr. Justice Krever testified that the Royal Commission's ability to apply for search warrants was crucial to their investigation.

The findings of the Royal Commission were published in three volumes.[13] The volumes contain tremendous detail about the investigative companies, insurance companies, and other institutions that worked together to acquire health records through surreptitious and illicit means.

So many insurance companies were found to have been using health information obtained under false pretenses that the Insurance Bureau of Canada made a general admission to the Royal Commission that its members had gathered medical information through various sources without the authorization of the patient. Many members of the Insurance Bureau of Canada are subsidiaries of American insurance companies. Some investigative agencies that obtained information under false pretenses are also subsidiaries of American companies.[14]

Mr. Justice Krever testified that he was "very much surprised"[15] by the abuses of health information that the Royal Commission uncovered. **He also testified that he suspected that the practices occurred not only in Ontario but throughout all of North America.**[16]

---

[13] Report of the Commission of Inquiry into the Confidentiality of Health Information (1980) (Ontario, Canada).
[14] *Privacy of Medical Records*, Hearings before a Subcomm. of the House Comm. on Government Operations, 96th Cong., 1st Sess. 538-41, 549-51 (1979).
[15] Id. at 543.
[16] Id. at 508, 511.

Because of the similarities between the Canadian and American casualty insurance industry and the private investigation industry, **the House Government Operations Committee inferred in a 1980 report that the same techniques for acquiring health information that were used in Canada were also used in the United States.** The techniques used by the Factual Services Bureau were identical to those common in Canada. All of the people involved in the Denver and Canadian investigations have stated their view that the practices were common throughout the United States.[17]

More U.S. Evidence

The Institute of Medicine (IOM) also expressed alarm about the acquisition and use of medical information through illegal or unethical means.[18]

The House Committee reached this conclusion in 1994:

> Based on past investigations and on more recent evidence of widespread, legal and illegal buying and selling of personal information protected by law, the Committee sees no reason to change the 1980 conclusion that there is routine trafficking in health records in the United States. If anything, organized trafficking in personal records, both legal and illegal, may have increased in the last fifteen years.

The extent to which surreptitious trafficking in medical information continues today is unknown. No recent investigative work in this area has been conducted. As the Krever Commission documented, a proper investigation may require significant powers to compel and seize documents.

There are at least four reasons to believe that the congressional findings from 1980 and 1994 about surreptitious trafficking in medical information are still valid today. First, the demands for information have not changed. Insurers, employers, and lawyers continue to find medical information useful. Second, sources of medical information have multiplied in recent decades. A hospital or physician record is not the only source of detailed medical information. Much of the same information can now be found in the files of health insurers, managed care organizations, pharmacy benefit managers, disease management companies, and others who collect and obtain patient information in the routine course of their activities. Thus, there are more potential suppliers of information than in the past. Third, illicit trafficking in other forms of personal information – including bank and telephone records – appears to have expanded in recent years.[19] Fourth, a 2006 United Kingdom investigation found the same types of surreptitious trafficking in personal information that earlier investigations uncovered in the United States and in Canada. Given past history, it is hard to believe that trafficking in health

---

[17] See Comm. on Government Operations, H.R. Rep. No. 96-832, Part I, 96th Cong., 2d Sess. 27 (1980) (report to accompany H.R. 5935).

[18] Institute of Medicine, Health Data in the Information Age: Use, Disclosure, and Privacy 160-161 (1994).

[19] See, e.g., *Phone Records for Sale: Why Aren't Phone Records Safe From Pretexting?*, Hearing before the House Comm. on Energy and Commerce (Feb. 1, 2006) (Testimony of Marc Rotenberg, Executive Director, Electronic Privacy Information Center), http://www.epic.org/privacy/iei/pretext_testimony.pdf.

records has disappeared while trafficking in other records continues.

2006 Report from the UK

A 2006 report from the United Kingdom Information Commissioner also provides evidence that surreptitious trafficking in personal information continues. The report is *What Price Privacy? The Unlawful Trade in Confidential Personal Information*.[20]

The 2006 UK report is based on investigative work done by the Information Commissioner's Office (ICO) and the police. In the introduction to the report, the Information Commissioner said:

> Personal information has a value – whether it is the embarrassing secret of a celebrity, a politician or someone else in the public eye, or the whereabouts of a private individual who it is thought owes some money. All cases in this illegal trade share in common that they involve personal and private information, and that the organisation holding the information has not authorised its disclosure. Usually stored on computer, these are the jigsaw pieces which help to build up a picture of each one of us as a unique individual. The trade in such information represents so serious a threat to individual privacy that this is the first report I or any of my predecessors have presented to Parliament under the Act's special powers.

The findings of the report suggest that the surreptitious trafficking in personal information in Great Britain is similar to the documented activity in the United State and Canada.

> 1.2 This report reveals evidence of **systematic breaches in personal privacy that amount to an unlawful trade in confidential personal information**.
>
> 1.7 Much more illegal activity lies hidden under the surface. Investigations by the ICO and the police have uncovered evidence of **a widespread and organised undercover market in confidential personal information**. Such evidence forms the core of this report, providing details about how the unlawful trade in personal information operates: who the buyers are, what information they are seeking, how that information is obtained for them, and how much it costs.
>
> 1.9 The personal information they are seeking may include someone's current address, details of car ownership, an ex-directory telephone number or records of calls made, bank account details or **intimate health records**.
>
> 1.10 The 'suppliers' almost invariably work within the **private investigation industry**: private investigators, tracing agents, and their operatives, often working loosely in chains that may include several intermediaries between ultimate customer and the person who actually obtains the information.

[20] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/what_price_privacy.pdf.

1.11 **Suppliers use two main methods to obtain the information they want: through corruption, or more usually by some form of deception**, generally known as 'blagging'. Blaggers pretend to be someone they are not in order to wheedle out the information they are seeking. They are prepared to make several telephone calls to get it. Each call they make takes them a little bit further towards their goal: obtaining information illegally which they then sell for a specified price. Records seized under search warrants show that many private investigators and tracing agents are making a lucrative profit from this trade.

4.5 In September 2000, the Information Commissioner's predecessor joined forces with the Benefits Agency and the Inland Revenue in a concordat known as BAIRD. The aim was actively to investigate people and organisations suspected of systematically and unlawfully obtaining personal information from the two agencies and selling it on to clients. The BAIRD team **detected over 100,000 offences**, leading to a number of successful prosecutions.

The UK report also confirmed the difficulty of uncovering trafficking in personal information and the value of search warrants in finding evidence:

5.1 While the ICO had long suspected the existence of an organised trade in confidential personal information, **charting the full extent of any unlawful activity is naturally fraught with difficulty**. An insight into the scale of this unlawful market came in late November 2002 when the ICO was invited to attend **a search of premises in Surrey executed under warrant** by the Devon & Cornwall Constabulary. The raid concerned the suspected misuse of data from the Police National Computer (PNC) by serving and former police officers. Recognising the significance of documents listing vehicle registration numbers, the ICO investigating officer was able to link the apparently random numbers to vehicle checks carried out within the Driver and Vehicle Licensing Agency (DVLA) by two officials. Corruption was the stark conclusion and two investigations were subsequently launched: the ICO's Operation Motorman into data protection offences and later Operation Glade by the Metropolitan Police into possible corruption by police officers or civilian police employees.

The insurance industry was also a prime customer for the information in the UK just as was the case in Canada.

5.12 **The insurance industry is another sector with an apparent incentive to acquire confidential personal data, particularly in respect of suspect claims.** An insurance company with evidence of fraud might try to argue that its activities were necessary for preventing or detecting crime. But it would still have to prove that the activity was 'necessary' (implying that no other reasonable means were readily available) and that there was, in fact, a 'crime'. The mere possibility that an offence might have been committed would not provide a sufficiently robust defence, without corroborating evidence.

Others who sought personal information included reporters and debt collectors.

Some of the report's conclusions:

> 7.1 **Evidence collected by the ICO points to a flourishing and unlawful trade in confidential personal information by unscrupulous tracing agents and corrupt employees with access to personal information.** Not only is the unlawful trade extremely lucrative, but those apprehended and convicted by the courts often face derisory penalties. The situation is already serious and underlines the need for stronger sanctions against those who breach the Data Protection Act 1998. The Government's plans for increasingly joined up and e-enabled public sector working make the change even more urgent.

It is worthy of observation that the UK has a comprehensive data protection law. That law has not provided much of a barrier to surreptitious trafficking in personal information. The Information Commissioner's report recommends stiffer criminal penalties, including prison sentences, for offenders.

HIPAA Doesn't Help Much

Recent U.S. legislation on health privacy has limited and uncertain effect. The Health Insurance Portability and Accountability Act (HIPAA)[21] includes a federal criminal penalty for the wrongful disclosure and wrongful obtaining of individually identifiable health information.[22] While the penalties are substantial, the Department of Justice has limited the application of the criminal penalties so that many individuals who work in health care and health insurance facilities cannot be prosecuted under HIPAA for selling patient records.

In a 2005 opinion by the Office of Legal Counsel, the Department[23] concludes that only covered entities (most health care providers, all health plans, and all health care clearinghouses) under the HIPAA privacy rule[24] can be prosecuted for criminal violation of the Act. A physician may be criminally liable for trafficking in health records, but a hospital clerk or orderly may not be prosecuted under HIPAA for the same conduct. **Professor Peter Swire, chief counselor for privacy in the Clinton Administration, called the OLC opinion as "bad law and bad policy."**[25]

A later unofficial article by Assistant United States Attorney Peter Winn suggests that there other criminal statutes might be used to prosecute some people who do not fall within the OLC-defined scope of HIPAA.[26] Winn discusses 18 U.S.C. § 2, a statute that establishes a

---

[21] Public Law 104-191 (1996).
[22] 42 U.S.C. §1320d-6.
[23] *Scope of Criminal Enforcement Under 42 U.S.C. § 1320d-6*, http://www.usdoj.gov/olc/hipaa_final.htm (June 1, 2005).
[24] 45 C.F.R. Part 164
[25] See Peter Swire, *Justice Department Opinion Undermines Protection of Medical Privacy* (June 7, 2005), http://www.americanprogress.org/site/pp.asp?c=biJRJ8OVF&b=743281
[26] Peter Winn, *Criminal Prosecutions under HIPAA*, 53 United States Attorneys' Bulletin 21 (2005), http://www.usdoj.gov/usao/eousa/foia_reading_room/usab5305.pdf.

criminal penalty covering any person who willfully causes an act which, if performed by another, would be a criminal offense.[27] In other words, if a person is not capable of committing a violation under a criminal statute, that person can nevertheless be liable criminally for an act that would have been a crime if committed by the person's principal. In a HIPAA case, a hospital worker who is not a covered entity who sells a patient record could be criminally liable under 18 U.S.C. § 2 because the sale would violate HIPAA if done by the covered entity that is the worker's employer. **However, this theory would not cover the purchaser of the patient record.**

While there have now been a few post-HIPAA prosecutions of individuals within the health care system for criminal disclosures, no person such as a investigator, insurance company, or employer who has improperly obtained health records has been prosecuted under the HIPAA criminal penalty. It remains far from certain that the HIPAA criminal penalty will be an effective deterrent against trafficking in health information.

2006 UK Update

The UK Information Commissioner issued a report updating activities on pretexting six month after the earlier report. The report is titled *What Price Privacy Now? The First Six Months Progress in Halting the Unlawful Trade in Confidential Personal Information*.[28]

The updated report shows that events have further highlighted the illegal trade in confidential personal information. In the new report, the Information Commission published a list of publications (newspapers and magazines) that the previous investigation identified as buyers of records obtained through pretexting. The three top publications identified were the Daily Mail (952 transactions), Sunday People (802 transactions), and Daily Mirror (681 transactions). The report also provides details on the responses of groups representing journalists, publishers, investigators, insurers, bankers, and others.

The report concludes:

> We are pleased that the report and the issues it raises have been widely circulated by professional bodies, trade associations and others. Whilst some responses may be a little disappointing **most organisations we have contacted have commendably taken further steps to stifle the illegal trade in confidential personal information**, for example by amending their codes or producing guidance. We will draw the Government's attention to the calls from some of those bodies for better legal access to relevant information in particular to trace absconded debtors.

---

[27] 18 U.S.C. § 2. Principals

(a) Whoever commits an offense against the United States or aids, abets, counsels, commands, induces or procures its commission, is punishable as a principal.

(b) Whoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal.

[28] http://www.ico.gov.uk/upload/documents/library/corporate/research_and_reports/ico-wppnow-0602.pdf.

There is still further work to be done to reduce the demand for illegally obtained confidential information. This work will be ongoing. We will continue to track down and prosecute offenders. We will continue to press the Government to introduce the option of a prison sentence and see this progress report as supporting that goal. We will continue to raise awareness and we will encourage and work with any organisation that wants to raise standards or produce clear guidance on data protection obligations. In particular we will be working closely with the media on the development of relevant guidance and standards for journalists.

#####