No. 07-1945

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

_____

IMS HEALTH INCORPORATED, A DELAWARE CORPORATION;
VERISPAN, LLC, A DELAWARE LIMITED LIABILITY COMPANY;

Plaintiffs – Appellee,

v.

KELLY A. AYOTTE, ATTORNEY GENERAL FOR THE STATE OF NEW HAMPSHIRE,

Defendant – Appellant.

_____

ON APPEAL FROM THE UNITED STATES DISTRICT COURT FOR
THE DISTRICT OF NEW HAMPSHIRE

_____

SUPPLEMENTAL BRIEF FOR THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* AND 16 EXPERTS IN PRIVACY LAW AND TECHNOLOGY IN SUPPORT OF DEFENDANT – APPELLANT KELLY A. AYOTTE, URGING REVERSAL

MARC ROTENBERG
1st Cir. Bar No. 120921
Counsel of Record
MELISSA NGO
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
(202) 483-1140

August 20, 2007

TABLE OF CONTENTS

TABLE OF AUTHORITIES.....ii

CORPORATE DISCLOSURE STATEMENT.....iv

STATEMENT OF AMICI.....v

ARGUMENT.....1

I. Medical Privacy is a Fundamental Concern for Patients.....1

II. The New Hampshire Prescription Confidentiality Act Advances a Substantial State Interest in Privacy Protection.....3

III. IMS Health's "De-identification" Practices Do Not Obviate the Medical Privacy Interests of New Hampshire Residents.....6

CONCLUSION.....11

CERTIFICATE OF COMPLIANCE WITH RULE 32(a).....12

CERTIFICATE OF SERVICE.....13

TABLE OF AUTHORITIES

CASES

Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y., 447 U.S. 557 (1980) 4

IMS Health, Inc. v. Ayotte, Civ. No. 06-cv-280-PB, 2007 WL 1244077 (D.N.H. filed Apr. 30, 2007) 7, 8

Northwestern Memorial Hospital v. Ashcroft, 362 F.3d 923 (7th Cir. 2004).....5

STATUTES

Prescription Restraint Law, 2006 N.H. Laws 328, codified as N.H. Rev. Stat. Ann. §§ 318:47-f & 318:47-g & 318-B:12, IV (2006).....4

HIPAA Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. §§ 160.103 & 164.514(b)(2) (2006).....8

OTHER AUTHORITIES

Amended Joint Stipulation of Facts (trial document 88) 1

David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, U. CHI. LEGAL F. 139 (1996).....5

Harris Interactive, *HIPAA Notices Have Improved Public's Confidence That Their Medical Information is Being Handled Properly: However public split on benefits of and privacy risks associated with Electronic Medical Records*, Feb. 24, 2005.....1

Jerry Kang, Prof., *Cyberspace Privacy*, 50 Stan. L. Rev. 1193 (Apr. 1998) 5

Joe Mullin, *States consider limits on medical data-mining*, Boston Globe, Apr. 7, 2007.....2

Khaled El Emam et al., *Evaluating Common De-identification Heuristics for*

Personal Health Information, 8 J. Med. Internet Res. (2006).....9

Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality,* 25 J. Law, Med., & Ethics (1997).....*passim*

Latanya Sweeney, *Roundtable Discussion: Identifiability of Data*, Subcomm. on Privacy and Confidentiality, Nat'l Comm. on Vital and Health Statistics, Jan. 28, 1998….....7

Magdalene Perez, *Patient info for sale*, Newsday, June 19, 2007.....2, 9

Nat'l Physician's Alliance, *Issue Brief: The Sale of Physician Prescribing Data Raises Health Care Costs*.....2, 3

Salvador Ochoa et al., *Re-identification of Individuals in Chicago's Homicide Database: A Technical and Legal Study*, Massachusetts Institute of Technology (2001). 6, 9

Steve Bailey, *Your Data for Sale?*, Boston Globe, Mar. 24, 2006.....10

Tanya Alberts, *Doctors ask AMA to assure some privacy for their prescription pads*, AMNews, Dec. 25, 2000.....2

CORPORATE DISCLOSURE STATEMENT

The Electronic Privacy Information Center ("EPIC") is a corporation with no parent corporation. No publicly held company owns 10% or more of the stock of EPIC.

STATEMENT OF AMICI

The Electronic Privacy Information Center ("EPIC") is a public interest research center in Washington, D.C., which was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values, including *Hiibel v. Sixth Judicial Circuit of Nevada*, 542 U.S. 177 (2004); *Doe v. Chao*, 540 U.S. 614 (2003); *Smith v. Doe*, 538 U.S. 84 (2003); *Department of Justice v. City of Chicago*; 537 U.S. 1229 (2003); *Watchtower Bible and Tract Society of N.Y., Inc. v. Village of Stratton*, 536 U.S. 150 (2002); *Reno v. Condon*, 528 U.S. 141 (2000); *Kohler v. Englade*, 470 F.3d 1104 (5th Cir. 2006); *United States v. Kincade*, 379 F.3d 813 (9th Cir. 2004), *cert. denied* 544 U.S. 924 (2005); and *State v. Raines*, 857 A.2d 19 (Md. 2003).[1]

At issue in this case are the privacy interests of New Hampshire residents that the state of New Hampshire sought to protect through the enactment of legislation. The state has a vital interest in regulating conduct that adversely affects the transfer and sale of computerized medical record information. Not only has Appellee IMS Health challenged this regulation as a violation of Appellee's right to profit from the sale of this sensitive data, Appellee engages in practices that continue to endanger the privacy interests of New Hampshire residents. Amicus

[1] IPIOP Clerks Caitriona Fitzgerald, Harley Geiger, Evan Mayor, Jennifer Shyu, and Aleah Yung assisted in the preparation of this brief.

therefore submits this brief to make clear the substantial interest in preserving this important state statute as well as the ongoing concern about the transfer of "de-identified" patient data to datamining firms. If this conduct is commercial speech, the lower court has missed a vital element of the governmental interest in regulating that speech, namely the privacy interests of patients. This brief shows that (1) the information is not truly anonymized; (2) as a result, there are real dangers to patient privacy in having this data trade, and therefore (3) the state interest in protecting patient privacy, ignored by the court below, requires reversal.

SIXTEEN LEGAL SCHOLARS AND TECHNOLOGY EXPERTS

John Anderson, Professor of Law, Shepard Broad Law Center, Nova Southeastern University, Fort Lauderdale, FL

Anita L. Allen, Professor of Law and Professor of Philosophy, University of Pennsylvania Law School, Philadelphia, PA

Ann Bartow, Professor of Law, University of South Carolina School of Law, Columbia, SC

Christine L. Borgman, Professor and Presidential Chair, Department of Information Studies, UCLA, Los Angeles, CA

James Boyle, Professor of Law, Duke Law School, Durham, NC

Dr. David Chaum, Founder, Punchscan, http://punchscan.org/

Philip Friedman, Friedman Law Offices, PLLC, Washington, DC

Deborah Hurley, Wayland, MA

Jerry Kang, Professor of Law, ULCA, Los Angeles, CA

Chris Larsen, CEO, Prosper Marketplace, Inc., San Francisco, CA

Mary Minow, LibraryLaw.com, Los Altos, CA

Dr. Peter G. Neumann, Principal Scientist, Computer Science Laboratory, SRI, Menlo Park, CA

Dr. Deborah Peel, Founder, Patient Privacy Rights, Austin, TX

Bruce Schneier, Chief Technology Officer, BT Counterpane, Mountain View, CA

Robert Ellis Smith, Publisher, Privacy Journal, Providence, RI

Frank M. Tuerkheimer, Professor of Law, University of Wisconsin, Madison, WI

ARGUMENT

I. Medical Privacy is a Fundamental Concern for Patients

There are approximately 1.4 million health care providers in the United States. These providers write billions of prescriptions each year for more than 8,000 different pharmaceutical products. Amended Joint Stipulation of Facts ¶ 9 (trial document 88). These prescriptions are filled at 54,000 retail pharmacies throughout the country. *Id*. The retail pharmacies acquire records for every prescription they fill. These records include: patient name; prescriber identification; drug name; dosage requirement; quantity; and date filled. *Id*. ¶ 13. In order to comply with federal and state privacy laws, patient identifying information is encrypted and de-identified, often with software installed by the datamining companies themselves. The rest of the prescription record remains intact. Thus, a patient's entire drug history is correlated, and each provider can be identified along with their prescribing habits. This practice raises privacy concerns for both patients and health care providers.

Public sentiment overwhelming favors the protection of patient privacy. Among the American public, 70% of the people have concerns over the sharing of their medical information without their knowledge.[2] At least one person has had her prescription information, including her name, Social Security number, and

[2] Harris Interactive, *HIPAA Notices Have Improved Public's Confidence That Their Medical Information is Being Handled Properly: However public split on benefits of and privacy risks associated with Electronic Medical Records,* Feb. 24, 2005.

medical conditions, sold to another pharmacy in a legal transaction without her knowledge or consent.[3] As a result of these findings, the states of New York, Nevada, Arizona, Illinois, Kansas, Maine, Massachusetts, Rhode Island, Vermont, Washington, West Virginia and Texas have considered bills banning the sale of prescriber-data.[4] The nation's first law banning prescriber-data is the focus in this case.

Doctors have also petitioned the American Medical Association (AMA) on behalf of themselves and their patients for legal relief, blaming data-mining companies for interfering with the patient-doctor relationship and violating doctor and patient privacies.[5] Even after the AMA adopted an opt-out approach to the sale of prescriber-data, doctors continue to question this practice and lobby for change.[6]

Although the AMA's Prescribing Data Restriction Program (PDRP) allows physicians to opt-out of having their prescribing history accessed by drug representatives, many physicians feel it is inadequate. The National Physician's Alliance supports a complete ban on the sale of prescriber-data.[7] They have spoken against the PDRP because the program is burdensome and not widely

---

[3] Magdalene Perez, *Patient info for sale,* Newsday, June 19, 2007.
[4] Joe Mullin, *States consider limits on medical data-mining,* Boston Globe, Apr. 7, 2007.
[5] Tanya Alberts, *Doctors ask AMA to assure some privacy for their prescription pads,* AMNews, Dec. 25, 2000.
[6] Joe Mullin, *States consider limits on medical data-mining, supra* note 4.
[7] Nat'l Physician's Alliance, *Issue Brief: The Sale of Physician Prescribing Data Raises Health Care Costs*, *available at* http://npalliance.org/images/uploads/IssueBrief-Prescribing_Data_low_res.pdf.

publicized. In its current form, the opt-out option is only valid for three years, at which time doctors are required to sign up again.[8]

Health care providers face the unique challenge of providing quality, affordable health care to all members of the population, while protecting each patient's fundamental right to privacy. The increasing dependence on electronic databases of patient information will meet many of these goals by reducing institutional costs, integrating applicable data from multiple sources, and allowing patients to receive a higher and more accurate level of care.[9] However, this transition to a centralized depository for health care information will require the sharing of private medical records with secondary actors, such as researchers, economists, statisticians, administrators, consultants, and computer scientists. Unfortunately, the current legal and security infrastructure surrounding patient medical information will not undergo a similar modernization for the electronic age. As a result, any system of electronic health care records or centralized health care database will lack proper privacy safeguards.

II. The New Hampshire Prescription Confidentiality Act Advances a Substantial State Interest in Privacy Protection

For reasons set forth above and in the brief of Appellant Kelly A. Ayotte, the Attorney General of New Hampshire, the New Hampshire legislature passed

---

[8] *Id.*

[9] *See* Latanya Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality,* 25 J. Law, Med., & Ethics, 98-99 (1997) (summarizing industry and research use of personally identifiable health care information).

House Bill 1346 to protect the privacy of patients, as well as to control health care costs, to protect the health and safety of New Hampshire citizens, and the privacy of doctors. House Bill 1346 is codified at N.H. RSA 318:47-f, RSA 318:47-g and RSA 318-B:12. *See* 2006 N.H. Laws 328. The relevant section of the Act states:

> Records relative to prescription information containing patient- identifiable and prescriber-identifiable data shall not be licensed, transferred, used, or sold by any pharmacy benefits manager, insurance company, electronic transmission intermediary, retail, mail order, or Internet pharmacy or other similar entity, for any commercial purpose, except for the limited purposes of pharmacy reimbursement; formulary compliance; care management; utilization review by a health car provider, the patient's insurance provider or the agent of either; health care research; or as otherwise provided by law. Commercial purpose includes, but is not limited to, advertising, marketing, promotion, or any activity that could be used to influence sales or market share of a pharmaceutical product, influence or evaluate the prescribing behavior of an individual health care professional, or evaluate the effectiveness of a professional pharmaceutical detailing sales force. . . . Nothing in this section shall prohibit the collection, use, transfer or sale of patient and prescriber de-identified data by zip code, geographic region or medical specialty for commercial purposes. . . .

N.H. RSA 318:47-f.

It is the provision of the Act that permits the transfer of "de-identified" patient data that gives rise to amicus's brief. Simply stated, amicus believes that the privacy interest that undergirds the state's interest in this statute is even greater than what the legislature recognized, and that the Court should give even greater weight to the *Central Hudson*, *Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of N.Y.*, 447 U.S. 557 (1980), substantial interest analysis if it concludes that the statute implicates speech interests.

As Judge Posner wrote for the court in *Northwestern Memorial Hospital v. Ashcroft*, 362 F.3d 923, 929 (7th Cir. 2004), a case involving access to redacted medical records:

> Even if there were no possibility that a patient's identity might be learned from a redacted medical record, there would be an invasion of privacy. Imagine if nude pictures of a woman, uploaded to the Internet without her consent though without identifying her by name, were downloaded in a foreign country by people who will never meet her. She would still feel that her privacy had been invaded. The revelation of the intimate details contained in the record of a late-term abortion may inflict a similar wound.

As Professor Jerry Kang has explained:

> [W]e must recognize that anonymity comes in shades. Although no specific individual is identified facially, the individual may be identifiable in context or with additional research. . . . Imagine that a psychiatrist publishes verbatim counseling notes in a best-selling book, but in a way that the specific identity of the patient cannot be determined. If the patient protests at having her story chronicled in agonizing detail to the public, could the good doctor respond that because the information is not identifiable to the specific patient, even with additional research, it is not "personal information." And, because it is not personal information, the patient lacks any privacy claim? To my mind, this reasoning fails to account for the residual privacy interest that exists, notwithstanding the anonymity.[10]

In similar fashion, there are important and distinct patient privacy interests to be considered in this case involving the transfer of "de-identified" personal information, that may in practice be re-identified or, even if not, may still affect a cognizable privacy interest. These interests are in addition to the privacy interests

[10] Prof. Jerry Kang, *Cyberspace Privacy*, 50 Stan.L.Rev. 1193, 1209 (Apr. 1998). *See also* David G. Post, *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity, and Limited Liability in Cyberspace*, U. CHI. LEGAL F. 139, 149-51 (1996) (discussing how context can sometimes provide identity information of facially anonymous e-mails).

of the doctor-patient relationship that are addressed in the brief of Appellant Ayotte.

III. IMS Health's "De-identification" Practices Do Not Obviate the Medical Privacy Interests of New Hampshire Residents

The plaintiffs, IMS Health Inc. and Verispan, LLC, are both datamining companies which purchase and compile prescription information in order to sell the data to research and academic institutions, as well as law enforcement agencies, and private organizations. Their biggest clients by far are pharmaceutical companies, which use the data extensively for "detailing," targeting doctors for office visits by sales representatives.

The patient data collected by IMS Health is not truly secure. Quasi-identifiers can be used for re-identification because they can be linked to external databases that contain identifying variables. This method, record linkage, occurs when two or more databases are joined. Such information can be obtained through public records, such as birth and death certificates.[11] Using record linkage, de-identified data can also be easily re-identified. For example, by utilizing date of birth, gender, and zip code information for members of the public, a researcher was able to uniquely identify 87% of the US population.[12]

---

[11] *See* Salvador Ochoa et al., *Re-identification of Individuals in Chicago's Homicide Database: A Technical and Legal Study*, Massachusetts Institute of Technology (2001) (utilizing the Social Security Death Index and de-identified information about Chicago homicide victims, the researchers were able to re-identify 35% of the victims).
[12] Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality* at 98-99, *supra* note 9.

It is easier to identify people who have a unique combination of quasi-identifiers compared to others in the population. For example, the sole female in a male dominated working group creates population uniqueness.[13] Similarly, when a person has unique quasi-identifiers compared with the rest of the individuals in the sample group, that person's sample is unique. This also makes the person easier to identify because the unique feature makes the person easier to trace in the real world. This can often be done without name, Social Security number, address, phone number, or other easily identifiable data.

Re-identification of data through record linkage creates additional problems for public figures about which more personally identifiable information is commonly known. For example, a former governor of Massachusetts had his full medical record re-identified after the researcher cross-referenced Census information with de-identified health data.[14] According to Latanya Sweeney, with birth date alone, 12% of a population of voters can be re-identified. With birth date and gender, that number increases to 29%, with birth date and zip code it increases to 69%, and with full postal code and birth date, 97% of people can be re-identified.[15] The ease with which records can be linked for re-identification purposes also creates unique problems for victims of harassment or domestic

---

[13] *Id.*
[14] Latanya Sweeney, *Roundtable Discussion: Identifiability of Data,* Subcomm. on Privacy and Confidentiality, Nat'l Comm. on Vital and Health Statistics, Jan. 28, 1998, *available at* http://npalliance.org/images/uploads/IssueBrief-Prescribing_Data_low_res.pdf.
[15] *See* Sweeney, *Weaving Technology and Policy Together to Maintain Confidentiality, supra* note 9.

violence. This is especially true because the abusers may have additional information that could lead to greater ease of re-identification, for example, knowledge of past illnesses and the time frame of their occurrence.

The court below notes that IMS Health "de-identifies" patient data.[16] However, no legal regulation defines how IMS Health must de-identify data nor is IMS Health legally required to de-identify. The closest governing regulation, the Privacy Rule of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), requires the removal of 18 specific identifiers that relate to patient identity, including geographic subdivisions smaller than a state, all elements of date (except year), biometric identifiers, Social Security and medical record numbers.[17] However, HIPAA does not cover pharmaceutical data-mining companies such as IMS Health and Verispan.[18]

In the absence of legal authority, IMS Health has voluntarily removed patient identifying information. IMS Health's prescriber-data includes information on the prescriber's identity, the dosage and strength of the drug, the quantity dispensed, the date of service and a unique patient identifying number. It does not

---

[16] *IMS Health, Inc. v. Ayotte*, Civ. No. 06-cv-280-PB, 2007 WL 1244077 at *1 (D.N.H. filed Apr. 30, 2007).
[17] The others are name, telephone and fax numbers, email addresses, health plan beneficiary numbers, account numbers, license and vehicle identifiers, device identifier and serial numbers, web URLs, IP addresses, full face photos and comparable images, and any unique identifying number, characteristic or code. 45 C.F.R. § 164.514(b)(2) (2006). Non-identifiable information would include ethnic origin, weight, age range, and height.
[18] Covered entities include health plans, health care clearinghouses, such as billing services and community health information systems, and health care providers (including pharmacies) that transmit health care data in a way that is regulated by HIPAA. As a result, a covered entity that utilizes Protected Health Information must de-identify it in the manner specified by the Privacy Rule, distribute it only to certain institutions if the data is considered a limited data set, or if the data fits neither category, the entity must comply with the disclosure and other provisions of the Privacy Rule. *See* 45 C.F.R. § 160.103 (2006).

appear to contain a patient's gender, zip code, or birth date – identifiers necessary for patient re-identification.[19] However, IMS Health "de-identifies" this data only in compliance with the objected-to New Hampshire law, and only for prescriptions that originate from a New Hampshire zip code.[20] Prescriber-data in other states may contain additional personal identifiers that can facilitate re-identification in the event of a security breach.

Although de-identification measures are increasingly innovative and computationally complex, patient data is still vulnerable to attacks because sophisticated re-identification programs are also being developed. Individuals can be re-identified using information such as zip code, date of birth, and gender and then comparing that data to publicly available information. Such information is easily accessible via birth and death records, incarceration reports, voter registration files, and driver's licensing information.[21]

Data re-identification has broad implications. It can be used for business purposes, as well as by individual citizens with the proper tools. Re-identification can also be used for many types of investigative reporting, especially investigations involving celebrities or politicians.[22] The information gleaned from health records could provide useful and potentially embarrassing reports. It can

---

[19] *IMS Health Inc.*, 2007 WL 1244077, at *1.
[20] *Id*. at *9.
[21] Khaled El Emam et al., *Evaluating Common De-identification Heuristics for Personal Health Information*, 8 J. Med. Internet Res. 4 (2006).
[22] Ochoa, *Re-identification of Individuals in Chicago's Homicide Database: A Technical and Legal Study, supra* note 11.

also be used by someone trying to identify a very small group of individuals with a similar characteristic. Re-identified data may also be useful in divorce proceedings or for perpetrators of crime who may have specific information on one particular individual that they can then use to identify that person's health records.

The final threat to patient privacy lies in the owners of large databases of medical data, as they look to turn this information into profit. A loophole in HIPAA gives pharmacies the ability to sell patient data to other pharmacies.[23] Academic hospitals are considering plans to sell aggregated patient data to government, pharmaceutical, and biotech companies, insurers, and publishers.[24] The state of Massachusetts had similar plans to sell its collection of patient data.[25] Even if privacy technology is adopted and the data is properly encrypted and de-identified, the transfer of such large databases poses significant privacy risks for patients. The substantial state interest in limiting the disclosure of this personal information, particularly for purely commercial purposes, is clear.

[23] Magdalene Perez, *Patient info for sale, supra* note 3.
[24] Steve Bailey, *Your Data for Sale?*, Boston Globe, Mar. 24, 2006.
[25] *Id.*

CONCLUSION

Given the ongoing concerns about patient privacy and the troubling practices that could arise from "de-identified" data, the judgment of the District Court should be reversed.

Respectfully submitted,

_____
MARC ROTENBERG
1st Cir. Bar No. 120921

MELISSA NGO
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
(202) 483-1140

Dated: August 20, 2007

CERTIFICATE OF COMPLIANCE WITH RULE 32(a)

Certificate of Compliance with Type-Volume Limitation,
Typeface Requirements, and Type Style Requirements

1. This brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 3,208 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2004 in Times New Roman, 14 point font.

Date: _____ _____

MELISSA NGO
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
(202) 483-1140

CERTIFICATE OF SERVICE

I HEREBY CERTIFY that two copies of the foregoing *amicus curiae* brief was this day sent by Federal Express to the office of the Clerk, and by regular mail to:

James P. Bassett, Esquire
Jeffrey C. Spear, Esquire
Orr & Reno
One Eagle Square
P.O. Box 3550
Concord, NH 03302-3550

Richard W. Head
Associate Attorney General
NH Department of Justice
33 Capitol Street
Concord, NH 03301-6397

Thomas R. Julin, Esquire
Patricia Acosta, Esquire
Michelle R. Milberg, Esquire
Hunton & Williams
1111 Brickell Ave, Suite 2500
Miami, FL 32405

_____

MELISSA NGO
Electronic Privacy Information Center
1718 Connecticut Ave. NW 200
Washington, DC 20009
(202) 483-1140

Dated: August 20, 2007