GENETIC DATABASES AND BIOBANKS: WHO CONTROLS OUR GENETIC PRIVACY?

Yael Bregman-Eschet*

ABSTRACT

In the past several years a growing number of private biotech companies have been collecting and storing our genetic information and bodily tissues and linking it to life-long medical histories. Many of these commercial companies have close relationships with the public sector: they rely on public institutions to get access to certain medical data and tissue samples, while the public sector relies on those companies for commercial exploitation of the research. Despite the unique nature of the information collected and the sensitivity of genetic databases, these private bio-libraries are largely unregulated in the United States.

This article examines who has control over the assembly, use, and dissemination of genetic information in various types of genetic databases (*e.g.*, public and private databases), and how this power should be managed based on its effects on the privacy and autonomy interests of individuals. The article analyzes three examples: the Icelandic Health Sector Database, the U.K. Biobank, and the operation of private, commercial bio-repositories in the United States. It further examines, via these three examples, the increased involvement of the private sector that collects and stores medical and genetic information and the growing partnerships between the private and public sectors in the genetic realm. This analysis reveals the potential abuses of our personal genetic information by those who have control over it, and the need to place limitations on the uses of this information. This article calls for the adoption of industry-wide fair information practices and proposes a set of fair information principles tailored to meet the specific privacy needs in the genetic realm.

* J.S.D. Candidate, Olin Fellow, University of California at Berkeley; J.S.M., Stanford University, 2004; LL.B., University of Haifa, Israel, 2002. I wish to thank Pamela Samuelson for her guidance in developing this article, and Paul Schwartz, Michael Birnhack, David Winickoff, Theo Bregman, and Gal Eschet for comments on earlier drafts of this article.

TABLE OF CONTENTS

INTRODUCTION

In 2000, two teams – one privately owned and the other publicly funded – announced of the mapping of the human genome.[1] In the wake of this scientific breakthrough, and the better understanding of various genetic disorders and physical and psychological traits that it promised, expectations for the development of new treatments and cures for various medical conditions has grown tremendously. The Human Genome Project was therefore accompanied by multiple superlatives: the genome itself was described as the "book of life" and the mapping of the human genome was compared to the search for the Holy Grail.[2] However, this new genetic research also posed a growing threat to personal privacy, as vast amounts of medical and genetic information could now be better understood, compiled, and linked together.

In this era of information technology, hospitals, research institutions, and other pharmaceutical and biotechnology companies are enabled to establish huge databanks containing the medical information of individuals, and then to link this data with sensitive genetic information. This massive compilation of medical data, linked to genetic material and information, notwithstanding its benefit to the provision of health care and the optimization of genetic research, poses significant privacy concerns. The fact that our private genetic information is often times out of our personal control, combined with the lack of adequate safeguards to ensure the privacy of this information by those who do control it, greatly increases these concerns.

---

[1] KEVIN DAVIES, CRACKING THE GENOME: INSIDE THE RACE TO UNLOCK HUMAN DNA (2nd ed., 2002); LORI B. ANDREWS, MAXWELL J. MEHLMAN, & MARK A. ROTHSTEIN, GENETICS: ETHICS, LAW AND POLICY, 31-33 (2002).

[2] THE CODE OF CODES: SCIENTIFIC AND SOCIAL ISSUES IN THE HUMAN GENOME PROJECT (Daniel J. Kevles & Leroy Hood, ed., 1992); and *also* RICHARD LEWONTIN, IT AIN'T NECESSARILY SO: THE DREAM OF THE HUMAN GENOME AND OTHER ILLUSIONS, 133-196 (2nd ed., 2001) (refuting the use of the Holy Grail metaphor).

Genetic databases,[3] biobanks,[4] and population databases are already here, most probably to stay. The United States, the United Kingdom, Iceland, and Estonia are some examples of countries in which genetic databases already exist or are currently being developed. Of these, there are different types of genetic databases with diverse goals at heart. Forensic,[5] military,[6] commercial,[7] and research databases,[8] are a few that come to mind. There are also various modes of control over genetic information: public, private, and a hybrid of the two – with the private sector relying on the public sector to get access to the data, and the public sector relying on the private one for commercial exploitation of the research.[9]

The Icelandic government, for instance, granted a private, for-profit company a 12-year license to create an electronic database of the medical records of the entirety of the Icelandic population, and authorized this company to link the electronic database consisting of detailed medical information to two additional databases:

---

[3] Genetic databases refer to the storage of genetic information obtained from the analysis of tissue samples. *See also* Jean E. McEwen, *DNA Databanks* in GENETIC SECRETS: PROTECTING PRIVACY AND THE CONFIDENTIALITY IN THE GENETIC ERA, 231 (Mark A. Rothstein, ed., 1997).

[4] Biobanks (also named DNA databanks) refer to databases in which the actual tissue samples are stored and not just the genetic information derived thereof. *See also* McEwen, *id*.

[5] An example of such forensic databases is the establishment of DNA Dragnets in order to facilitate the apprehension of criminals. *See also*, *infra* section II.A.

[6] The United States military is another example of a governmentally controlled biobank in which DNA samples of soldiers are being stored for the purpose of identifying the remains of missing soldiers. For further discussion *see* McEwen, *supra* note 3, at 239-240.

[7] The number of private, commercial biobanks consisting of DNA and tissue samples is rapidly growing. Examples of commercial companies running private biobanks include Genomics Collaborative Inc., Ardais Corporation, and DNA Sciences, Inc. Each of these companies holds thousands of samples which are being used for the companies' commercial gain. *See* Jocelyn Kaiser, *Population Databases Boom, From Iceland to the U.S.*, 298 SCIENCE 1158, 1159 (November 8, 2002); and *also* Robin Marantz-Henig, *The Genome in Black and White (and Gray)*, THE NEW YORK TIMES MAGAZINE, 47 (October 10, 2004).

[8] The Human Genome Diversity Project (HGDP) is a good example of a proposed DNA database for research purposes. The purpose of this worldwide project was to sample and archive human genetic diversity, and especially samples from indigenous populations "as the first step towards enormous leaps in our grasp of human origins, evolution, prehistory, and potential." This project had failed due to the resistance voiced by indigenous groups that dubbed the project as the "vampire project." Recently, however, attempts have been made to revive the HGDP by the National Geographic Society and I.B.M. *See* Jenny Reardon, *The Human Genome Diversity Project: A Case Study in Coproduction*, 31 SOCIAL STUDIES OF SCIENCE 357 (2001); Nicholas Wade, *Geographic Society Is Seeking a Genealogy of Humankind*, THE NEW YORK TIMES at A16 (April 13, 2005).

[9] Alan Petersen, *Securing Our Genetic Health: Engendering Trust in UK Biobank*, 27(2) SOCIOLOGY OF HEALTH & ILLNESS 271, 276 (2005).

Iceland's genealogical database and a genetic database created by the company itself. The United Kingdom is currently in the midst of establishing the world's largest biobank, with samples taken from 500,000 volunteers; the information collected will be linked to the medical records and other health and life-style information of the participants. And in the United States, private companies, such as Ardais Corporation and Genomics Collaborative are establishing huge, private bio-repositories containing tissue samples linked to medical information and history, collected directly from patients or received from hospitals.

The analysis of these three examples reveals the potential abuses of some of our most personal and sensitive information by both public and private entities, and suggests the need to establish industry-wide fair information practices that will address the specific problems that arise from the collection and storage of genetic information and the linkage of this information to other types of personal information. Moreover, the analysis of these three examples – the Icelandic Health Sector Database, the U.K. Biobank, and the operation of private, commercial bio-repositories in the United States – accentuates the need to redefine the status of those who control such sensitive information, preferably crowning them as trustees – not owners – of the medical and genetic information they collect and compile.

This article, hence, deals with the question of control. It examines who has control over the assembly, use, and dissemination of information from various types of genetic databases (*e.g.*, public and private databases), and suggests how this power might be managed, taking into account its effects on the privacy and autonomy interests of individuals. Three key terms are used throughout the article: genetic privacy, autonomy, and property rights. The term genetic privacy applies the concept of privacy to genetic-related findings and refers to the use of personal data derived

from one's genes.[10] Autonomy, or bioautonomy, is used to describe one's decisional power over her genetic information and the uses made of it.[11] Lastly, property rights are used to refer to interests in an object (in this article – one's genes, tissues, or information derived thereof) that are attached to it, and that can be traded.[12]

Part I will address the ongoing debate as to whether genetic information is in fact different from other types of medical information. It will explain the threats to personal privacy posed by the growing number of bio-repositories and by their linkage to other medical and genetic databases, particularly if owned by private entities. Part II will examine several public and private bio-repositories already existing in the United States, will explore some of the potential abuses of genetic information stored in large databases and databanks, and will explain the need for the implementation of fair information practices for the accumulation, use, access, and transfer of the genetic information stored in these databases.

Part III will use the Icelandic Health Sector Database as a case study to explore new collaborative enterprises between governmental and commercial entities and the merger of knowledge accumulated in public and private repositories. This part will identify the risks and benefits of such collaborations, and will compare the Icelandic model that is based on commercial exploitation, to that chosen in the United Kingdom, which is based on public ownership, concluding that the latter is a better

[10] Anita Allen portrays the term "genetic privacy" as consistent of four dimensional aspects: 1) informational privacy that relates to access to personal information; 2) physical privacy, which relates to access to persons and personal spaces; 3) decisional privacy, which relates to governmental or other third party interference with personal choices; and 4) proprietary privacy that relates to ownership interests in the human body. *See* Anita L. Allen, *Genetic Privacy: Emerging Concepts and Values*, in GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA, 33-34 (Mark Rothstein, ed., 1997).

[11] *See also* David E. Winickoff, *Governing Population Genomics: Law, Bioethics, and Biopolitics in Three Case Studies*, 43 JURIMETRICS JOURNAL 187, 189 (Winter 2003) (defining bioinformation as "phenotypic information drawn from medical records and genotypic information drawn from tissue samples").

[12] *See also* Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARVARD LAW REVIEW 2055, 2058 (2004) (defining "property" as "any interest in an object, whether tangible or intangible, that is enforceable against the world. From this perspective, property rights run with the object, and can be contrasted with contract rights, which bind only parties in privity").

formulation to protect the autonomy and genetic privacy of individuals. Finally, conclusions drawn from the Icelandic and British examples will be applied to the American landscape. The inductions made from the two foreign examples to the United States emphasize the need to place limitations and safeguards in the form of self-regulation that will address the specific privacy concerns raised in the information technology – genetic era. A set of fair information principles tailored to the specific concerns raised by genetic databases and biobanks is therefore suggested.

I. GENETIC DATABASES: A NEW THREAT TO PRIVACY?

Medical data is considered to be highly sensitive, personal information. According to the 9th Circuit "one can think of few subject areas more personal and more likely to implicate privacy interests than that of one's health or genetic make-up."[13] Despite the sensitive and personal nature of medical information, certain proponents of the free market – namely Richard Posner and Richard Epstein – call for open access to medical and genetic information in the name of economic efficiency.[14] However, open access to both medical and genetic information may have far reaching social implications in the form of social stigma and genetic determinism that may lead, for instance, to employment and insurance discrimination, which are socially as well as economically undesirable.[15] For this reason, the free market may fail to adequately protect medical privacy.[16] Medical information thus requires considerable privacy protection and confidentiality, a necessity long recognized by the Hippocratic Oath.[17]

---

[13] *Norman Bloodsaw v. Lawrence Berkeley Laboratory*, 135 F.3d 1260, 1269 (1998).

[14] *See* Richard A. Posner, *The Right of Privacy*, 12 GEORGIA LAW REVIEW, 393 (1978); and Richard A. Epstein, *The Legal Regulation of Genetic Discrimination: Old Responses to New Technology*, 74 BOSTON UNIVERSITY LAW REVIEW 1 (1994).

[15] Paul M. Schwartz, *Privacy and the Economics of Personal Health Care Information*, 76 TEXAS LAW REVIEW 1, 25-31 (1997); Allen, *supra* note 10.

[16] *See* Schwartz, *id.*, at 42-51 (indicating three main reasons for the market failure to adequately protect medical privacy: lack of public knowledge regarding the use and treatment of personal data; an agency problem; and a collective action problem); and more generally DANIEL J. SOLOVE, THE

Genetic information is a sub-class of medical information.[18] It includes information that may be retrieved from an individual's DNA that, with the growing understanding of the human genome and its mapping, may reveal three levels of sensitive information: personal information about the individual such as genes, traits, and predisposition to certain diseases; medical information about an individual's kinship that can be attributed to one's genes; and information about the heritage of the individual, *e.g.* the routes and origin of her ancestors.

Despite the sensitivity of the information which may be retrieved from one's DNA and tissue samples, the degree of privacy protection that should be granted to genetic information is disputed. Legal scholar George Annas considers genetic information to be especially sensitive medical information because of the different levels of personal information it may reveal: not only about the individual, but also regarding her relatives.[19] According to Annas, our DNA is a reflection of our "future

---

DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE, 81-87 (2004) (listing four misgivings of the market in protecting personal data: the limitations of contract law; problems with bargaining power; the one-size-fits-all problem; and inequalities in knowledge).

[17] The Hippocratic Oath was originally written approximately 2,400 years ago (400 B.C.E.) in ancient Greece, and it declares: "…What I may see or hear in the course of the treatment or even outside of the treatment in regard to the life of men, which on no account one must spread abroad, I will keep to myself, holding such things shameful to be spoken about." *See* http://www.pbs.org/wgbh/nova/doctors/oath_classical.html (last visited January 2006).

[18] Although not all genetic information is necessarily a secret (e.g., the color of one's eyes or hair), if privacy is conceptualized as more than the classical secrecy paradigm, as suggested by Solove, genetic information may be viewed as private information. SOLOVE, *supra* note 16, at 143 (stating that: "we must abandon the secrecy paradigm. Privacy involves an expectation of a certain degree of accessibility of information. Under this alternative view, privacy entails control over and limitations on certain uses of information, even if the information is not concealed."); and *also infra* notes 121-123 and the accompanying text, explaining the need for different levels of protection for genetic information according to the degree of sensitivity of the information.

[19] This special sensitivity arises, according to Annas, because genetic information encompasses in it private information about one's self, about our relatives, and is important to private decision-making. *See* George J. Annas, *Genetic Privacy: There Ought to Be a Law*, 4 TEXAS REVIEW OF LAW & POLITICS 9, 9-10 (1999). For the opposite view *see* George Poste, *Privacy and Confidentiality in the age of Genetic Engineering*, 4 TEXAS REVIEW OF LAW & POLITICS 25 (1999) (arguing that the distinction between genetic data and other classes of medical information is false); and *also* Thomas H. Murray, *Genetic Exceptionalism and "Future Diaries": Is Genetic Information Different from other Medical Information?* In GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA, 60 (Mark A. Rothstein, ed., 1997).

diaries," with the ability to reveal predisposition to illnesses, traits, and even life span.[20]

However, this "future diary" metaphor has been widely contested by others.[21] It has been argued, in contrast, that "genetic information is neither unique nor distinctive in its ability to offer probabilistic peeks into our future health,"[22] and that any potential difference between genetic information and other classes of medical information is at most that of degree, not of kind.[23] Others see genetic data as distinct from other types of medical information, but not unique.[24] Similarly, the 9th Circuit concluded, in a majority opinion, that a blood sample is not substantially different than fingerprinting,[25] although Judge Nelson, in dissent, argued that: "DNA genetic pattern analysis catalogs uniquely private genetic facts about the individual that should be subject to rigorous confidentiality requirements even broader than the protection of an individual's medical records," [26] thus differentiating genetic information from other classes of medical data or fingerprint records.[27]

---

[20] Annas, *id.*, at 11-12.

[21] *See* Douglas H. Ginsburg, *Genetics and Privacy*, 4 TEXAS REVIEW OF LAW & POLITICS 17 (1999) (arguing that the "future diary" metaphor does not hold: first because actual diaries are much more diverse than out our genetic makeup; and second because while diaries contain our thought on past occurring, our DNA can reveal us only probabilities); and *also* Murray, *supra* note 19; Allen, *supra* note 10, at 49-51; Pauline T. Kim, *Genetic Discrimination, Genetic Privacy: Rethinking Employee Protections for a Brave New Workplace*, 96 NORTHWESTERN UNIVERSITY LAW REVIEW 1497 (2002) (Suggesting a different metaphor that compares human genes to the raw material input into a production process) *id*., at 1532-1537.

[22] Murray, *supra* note 19, at 64.

[23] Ginsburg, *supra* note 21, at 18.

[24] Lawrence O. Gostin, *Health Information Privacy*, 80 CORNELL LAW REVIEW 451, 489-492 (1995).

[25] *See Rise v. State of Oregon* 59 F.3d 1556 (9th Cir., 1995) in which the majority concluded that obtaining a blood sample from a convicted felon or a sex offender is not substantially different from fingerprinting.

[26] *Id*. at 1569.

[27] *See also* Jeffrey S. Grand, *The Blooding of America: Privacy and the DNA Dragnet*, 23 CARDOZO LAW REVIEW 2277 (August 2000) (rejecting the analogy of genetic makeup to fingerprints as being too simplistic and stating that: "biological samples volunteered in DNA dragnets have the potential to reveal far more intimate information about the individual donor than a simple fingerprint.") *id.*, at 2288-2289.

When referring to genetic databanks, one must distinguish between two types of repositories.[28] The first is genetic databases, which consist of information derived from individual genetic material and DNA. The second type of genetic repositories – DNA banks or biobanks – is a collection of tissue samples, such as blood, saliva, or hair, from which our DNA can be derived. Both types of banks pose potential threats to privacy: genetic databases do so via the accumulation of genetic information in one electronic form, and DNA banks do so by allowing for the possibility of making endless amounts of DNA copies for different uses from one single sample.

Computerization is one of the greatest challenges to medical privacy, genetic privacy included, in the information technology age.[29] The computerization of medical records makes the medical process more efficient, optimizes health care, and enhances research.[30] But the compilation of such vast amounts of sensitive data, in the form of medical and genetic information, in a single electronic database to which numerous people in different locations have access, also undermines personal privacy.[31]

---

[28] Murray, *supra* note 19, at 63-64; McEwen, *supra* note 3; Human Genetics Commission, *Inside Information: Balancing Interests in the Use of Personal Genetic Data*, summary report 12-13, 31 (May 2002) (hereinafter: U.K. Human Genetics Commission) at http://www.hgc.gov.uk/UploadDocs/DocPub/Document/insideinformation_summary.pdf (last visited January 2006).

[29] Mark A. Rothstein, *Medical Privacy – an Oxymoron?* NEWSDAY A25 (March 15, 1999). *See also* SOLOVE, *supra* note 16, at 2-4 (2004) (discussing the problems of digital dossiers).

[30] *See* Gostin, *supra* note 24; Poste, *supra* note 19; and *also* Schwartz, *supra* note 15, at 12-15.

[31] Gostin, *id.*, at 467-468; and *also* the United States Supreme Court's decision in *Whalen v. Roe* acknowledging "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *Whalen v. Roe* 429 U.S. 589, 605 (1977). *See also* SOLOVE, *supra* note 16, at 131-132. For a more general description of the benefits as well as the privacy threats associated with the Global Information Infrastructure *see* Larry Irving, National Telecommunications and Information Administration, *Introduction to Privacy and Self-Regulation in the Information Age* (June 1997), available at http://www.ntia.doc.gov/reports/privacy/intro.htm (last visited January 2006) (stating that: "The Global Information Infrastructure has tremendous potential to bring economic, social and cultural benefits to America and its citizens. Because it will facilitate and expand the flow of information between people and from place to place, the GII promises enhanced educational and employment opportunities, greater citizen participation, and improved delivery of government services. Information technologies promise to revolutionize the manner in which commerce is transacted domestically and across international borders. The GII has provided faster, cheaper, and more reliable communication of business data, so that great distances and multiple time zones are no

Biobanks, on the other hand, create a somewhat different challenge, particularly to the privacy and autonomy of the individual. The ability to store tissue and DNA samples for long periods of time and the possibility to create endless number of DNA copies from a single sample, give rise to the concern that these samples could be used in the future for purposes other than those for which they were originally intended.[32] For instance, stored tissue samples, collected before genetic testing was even available, can now be used to create DNA databanks for research purposes.[33] The U.K. Human Genetics Commission, for example, found it acceptable to use, for research purposes, old collections of samples for which informed consent was not sought, as long as the samples were anonymized.[34]

Alternatively, many biobanks ask their research subjects for open-ended permission to use their genetic information for future research.[35] This type of broad permission is a weak form of consent. It is weak because the research subject provides consent without being aware of the specific uses for which the samples might be used, or of possible future uses, which are yet unknown.[36] Genuine informed consent can only be granted if the research subjects understand and agree to the general nature of

---

longer barriers to transacting business. But while information technologies can bring these benefits to Americans, they also present new challenges to individual privacy. Not only does the GII make the collection, storage, and transmission of large amounts of personal data possible, use of the GII creates information trails that, without proper safeguards, could reveal the personal details of people's lives. Failure to recognize and protect the privacy interests could slow the growth of the GII. If we are to realize the full potential of the information infrastructure, the legitimate privacy interests of users of the GII must be acknowledged and protected").

[32] Annas, *supra* note 19, at 13-14. Such use if unauthorized by the individual who gave the sample will theoretically require additional consent from the patient.

[33] Gostin, *supra* note 24, at 467-468.

[34] U.K. Human Genetics Commission, *supra* note 28.

[35] ELISA EISMAN ET AL., CASE STUDIES OF EXISTING HUMAN TISSUE REPOSITORIES: "BEST PRACTICES" FOR THE GENOMIC AND PROTEOMIC AGE, chapter seven: Privacy, Ethical Concerns, and Consent Issues, 121, 132-135 (2003), available at http://www.rand.org/pubs/monographs/2004/RAND_MG120.pdf (last visited January 2006); David E. Winickoff & Richard N. Winickoff, *The Charitable Trust as a Model for Genomic Biobanks*, 349(12) THE NEW ENGLAND JOURNAL OF MEDICINE 1180, 1180-1181 (September 18, 2003).

[36] Winickoff & Winickoff, *id*.

the research, are asked for additional consent if different purposes are sought in the future, and have the power to oppose specific uses.[37]

Similar concerns, and in particular the inability to fully consent to future research techniques and uses, brought the United States military, for instance, to propose a fifty-year limitation on the length of time that blood and saliva samples (which are collected from military personnel to facilitate the identification of missing soldiers) are kept.[38] In addition, soldiers who leave the service can request the destruction of the samples collected by the military. The issue of long term sample storage was raised following the voicing of concerns that the military could potentially make additional, unauthorized uses of the genetic information collected, such as a "dragnet" for detecting criminals, or to determine predisposition to homosexual behavior.[39]

The privacy and autonomy threats, which accompany the information technology age and its mega databases that hold immense amounts of personal information, are not necessarily new. Nonetheless, the challenges of protecting medical and genetic privacy have been growing. One reason is the linkage made between medical information and the two types of genetic banks – genetic databases and biobanks. This linkage, which is increasingly being implemented to facilitate scientific progress, creates – absent sufficient safeguards – new dimensions to the existing privacy concerns relating to medical and genetic information.

Second, the private sector, is becoming increasingly involved in the collection and assembling of medical and genetic information and in linking it together, both

---

[37] *See generally,* SOLOVE, *supra* note 16, at 86 (stating that "a more complete range of choices must permit individuals to express their preferences for how information will be protected, how it will be used in the future, and with whom it will be shared."); and *also* U.K. Human Genetics Commission, *supra* note 28, at 10-11.

[38] McEwen, *supra* note 3, at 239-240; Annas, *supra* note 19, at 14.

[39] McEwen, *id.*, at 239-240.

independently and through collaborative work with governmental or research institutions, which willingly transfer individuals' genetic material and/or information to the hands of the private sector.[40] This partnership between the public and private sectors is evident in the Icelandic model, as well as from private agreements between hospitals and commercial biotech companies in the United States.

Although, the involvement of the private sector is crucial for efficient technological development,[41] the growing control that the private industry has over personal medical information and genetic material is problematic. First, unlike the public and non-profit sectors, whose primary goals should be increasing the pubic welfare, the private sector is primarily concerned with its own financial gains and the maximization of shareholder profits. Because of this, the danger exists that, absent adequate safeguards, the private sector may misuse this sensitive information in times of economic crises, such as selling the information in the event of bankruptcy.[42] The existing legal protection for medical and genetic information is insufficient to prevent this type of conduct that undermines the research subjects' genetic privacy and interests.[43]

Third, absent sufficient restrictions and guidelines for the storage of genetic information, each company is free to choose the levels of security granted to genetic information. As a result, we are witnessing incoherency in the manner in which sensitive information is stored and handled, a phenomenon that not only undermines

[40] For the history of public-sector and private-sector databases and the flow of information between the two,*see generally* SOLOVE, *supra* note 16, at 13-21.

[41] The race between private company Celera Genomics and the publicly funded Human Genome project, which dramatically accelerated the sequencing of the human genome, is a good example. Due to the involvement of a private company and the competition it entailed, 90% of the sequencing was reached 5 years before the original end date. *See* DAVIES, *supra* note 1.

[42] *See also infra* section II.C.5.

[43] *See also* the U.K. Human Genetics Commission, *supra* note 28, at 8-9.

the privacy interests of the research subjects, but is also viewed as placing greater difficulties in the conduct of the research.[44]

The growing control that private commercial companies have over our medical and genetic information and material; the lack of sufficient safeguards in place to protect personal privacy; and potential partnerships between the public and the private sectors that bestow additional power to the hands of the private sector, all intensify the threat to our autonomy and genetic privacy. Hence, this article calls for greater caution in the collection and usage of genetic information and material and its assembling with other types of medical information, and encourages the industry to embrace industry-specific fair information practices that will put limitations and restrictions on the compilation and usage ofgenetic data.

II. GENETIC DATABASES IN THE PUBLIC AND PRIVATE SECTORS

A. Public Sector Bio-Repositories

The public sector is probably the primary collector of genetic material. The largest collection of blood and tissue samples in the United States, as well as in the world, currently belongs to the National Pathology Repository of the Armed Forces Institute of Pathology (AFIP), where 92 million human specimens dating back to 1864 are held.[45] The British government plans to establish the world's largest biobank with blood and tissue samples taken from 500,000 volunteers, linked to their medical information and history.[46] It is not surprising, therefore, that most privacy concerns are directed towards the government and its control over this sensitive data. Most often the concerns regarding genetic privacy are being raised in the criminal context

[44] *See infra* note 138.
[45] *See* the Armed Forces Institute of Pathology website at http://www.afip.org/Departments/repository/npr.html (last visited January 2006); and EISMAN ET AL., *supra* note 35, at 161.
[46] *See* http://www.ukbiobank.ac.uk/about/overview.php (last visited January 2006).

and pertain to the creation of forensics databases, "DNA dragnets," and the fear that they will be used in a racial or discriminatory manner.[47]

The term “DNA dragnet” describes the collection of biological samples, such as blood or saliva, from individuals not specifically suspected of a crime.[48] These samples are thereafter used to create DNA profiles thatare compared to the profile of the suspect, which is based on evidence from the crime scene.[49] The first DNA dragnet was used in England in the late 1980s following a rape and murder case. In the course of the attempts to apprehend the perpetrator, 4,500 blood samples from males were collected and assembled by the police, until eventually the suspect was caught.[50] Today, such DNA dragnets are created and used throughout the world.[51]

San Diego was the first jurisdiction in the United States to establish a DNA dragnet in the early 1990s, collecting blood and saliva samples from hundreds of volunteers, in order to catch a serial killer who was believed to be African-American.[52] In fact, one of the primary purposes of these DNA dragnets is to expose those who refuse to participate in the sample collection. Despite the voluntary nature of participation in a DNA dragnet, refusal to take part in the collective efforts to find the suspect immediately raises police suspicion.[53] Today, most states have a system of DNA dragnets, and the specimens collected may be kept by the state indefinitely, even though the majority of the samples are taken from law-abiding citizens.[54] Many fear that these sample collections that contain the participants' DNA may be exploited

---

47 Many of the DNA dragnets involve suspects belonging to a racial group such as African-Americans. *See* for example, Grand, *supra* note 27, at 2278-2280; and *also* Marantz-Henig, *supra* note 7.
48 Grand, *id.*, at 2279-2280, 2282-2284.
49 Grand, *id.*, at footnote 1.
50 Grand, *id.*, at 2285; DANIEL J. SOLOVE & MARC ROTENBERG, INFORMATION PRIVACY LAW, 267-268 (2003).
51 Including the United Kingdom, Germany, France, Australia, and the United States. *See* Grand, *id.*, at 2285.
52 *See also* Grand, *id.*, at 2278-2279.
53 *See* Grand, *id.*, at 2282-2284; and SOLOVE & ROTENBERG, *supra* note 50, at 274.
54 Grand, *id.*, at 2279-2280.

in the future for uses other than the identification purposes they were originally intended for.[55]

In addition, DNA samples are now routinely collected by the state from people convicted of crimes such as rape and murder, or even people charged with misdemeanor crimes. Moreover, some states allow the collection of DNA samples from those merely arrested and not yet convicted of a crime.[56] The DNA Identification Act of 1994 authorizes the FBI to establish the national DNA database CODIS (Combined DNA Identification System). The CODIS database allows states to share and compare their DNA databases, thus increasing the efficiency and probability of solving crimes, but also undermining the privacy interests of those whose DNA samples have been collected and stored, and who are not necessarily convicted of any crime.

One of the major privacy concerns associated with these bio-collections is the possibility of unauthorized or unintended dissemination and use of the stored samples.[57] For instance, data collected from criminals could potentially be used for the study of genetic disposition for violence,[58] or genetic samples collected from military personnel could be used to identify men thought to be predisposed to homosexual behavior.[59]

Various legal measures taken in the United States attempt to address these fears in the public sector. Participants in public sector DNA collections are protected by the constitutional right to privacy,[60] the Fourth Amendment (in cases of

---

[55] U.K. Human Genetics Commission, *supra* note 28, at 12-13.
[56] McEwen, *supra* note 3, at 232-238.
[57] McEwen, *id.*, at 236-240.
[58] McEwen, *id.*, at 237-238. For more on the potential threats of studies on genetic determinism and predisposition for violence behavior conducted in prisons *see* Garland E. Allen, *Modern Biological Determinism: The Violence Initiative, The Human Genome Project, and the New Eugenics* in THE PRACTICES OF HUMAN GENETICS (Fortun & Mendelsohn eds., 1999).
[59] McEwen, *id.*, at 239-240.
[60] Grand, *supra* note 27, at 2309-2318.

unreasonable search or seizure),[61] the federal Protection of Human Subjects Rule (known as the "Common Rule"),[62] and the privacy rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[63] The existing system of checks and balances subjects "public" repositories of the Federal government and the states to increased scrutiny. For instance, by requiring that an Institutional Review Board (IRB) will oversee repository practices in the public sector and will insure that the privacy and confidentiality of research subjects are protected.[64] Yet, not all genetic databases and biobanks are under the control of the government, and the fear of misuse should not be directed at public repositories alone. In fact, there is a growing number of private, commercial repositories holding genetic material and information, which are not subject to the existing rules, and these tissue collections are growing rapidly. In just over five years commercial biotech companies managed to build private bio-repositories containing hundred of thousands of human tissue samples, many of which are unregulated.[65]

B. Commercial Databanks

In the past several years a growing number of commercial biotech companies in the United States have been collecting and storing personal genetic information and providing pharmaceutical companies and other research institutions for-a-fee access to their collections and bio-libraries. In fact, private biobanks may have an advantage

---

[61] *Id.*, at 2289-2309.

[62] 45 C.F.R §46. The Common Rule, which applies to research conducted by Federal agencies or using Federal money, provides regulations for human subject research and requires that the research subjects have a right to be removed from a repository if the information it stores is identifiable. *See also* EISMAN ET AL., *supra* note 35, at 140-141; Winickoff, *supra* note 11, at 191-192; and Grand, *supra* note 27 (suggesting that there is need for additional regulation for governmental retention of biological samples) *id.*, at 2318-2322.

[63] *See also infra* note 80 and the accompanying text.

[64] 45 C.F.R §46; *see also* EISMAN ET AL., *supra* note 35, at 126.

[65] *See also* EISMAN ET AL., *supra* note 35, at 168.

over public ones since they can more easily and quickly attract venture capital.[66] As a result, some academic medical centers have chosen, for financial reasons, to transfer their tissue samples to private commercial repositories.[67] These newly formed private bio-repositories yield various ethical challenges, including that of invasion of privacy.

Commercial biotech companies provide an array of private services and products including: paternity tests, genetic testing for predisposition for certain diseases and traits, genealogy and the tracing of origin and ancestry, [68] pharmacogenomics,[69] and even private forensics using DNA to establish profiles of crime suspects not matching any of the profiles in the Federal CODIS database. [70] DNAPrint Genomics is an example of such a private company providing all of the

---

[66] Winickoff & Winickoff, *supra* note 35, at 1183; and *also* U.K. Human Genetics Commission acknowledging that: "the development of medicines and treatments is largely a commercial undertaking and would be severely harmed if commercial access were denied." U.K. Human Genetics Commission, *supra* note 28, at 22.

[67] Winickoff, *supra* note 11, at 207-217.

[68] For instance, DNArints Genomics claims to be able to trace 85% of sub-Saharan Ancestry. *See* Marantz-Henig, *supra* note 7, at 50.

[69] Pharmacogenomics is a new strand of medicine based on genetics. It was made possible through the completion of the Human Genome Project and the human genome sequence. The use of genomics in the search for new therapeutic treatments, it is anticipated, will allow pharmaceutical companies to produce therapies better targeted to specific diseases. *See* Tanuja V. Garde, *Supporting Innovation in Targeted Treatments: Licenses of Right to NIH-Funded Research Tools*, 11 MICHIGAN TELECOMMUNICATIONS AND TECHNOLOGY LAW REVIEW 249, 252-253 (2005). However, one problematic phenomenon observed is the growing focus on what might be termed the genetics of race. The drug BiDil, for example, is to be the first "racial drug." The drug developed by NitroMed is approved for the treatment of heart failure exclusively in the African-American population after it was found to be unsafe for the general public. *See also* Marantz-Henig, *id.*; and Stephan Saul, *U.S. to Review Heart Drug Intended for One Race*, THE NEW YORK TIMES (June 13, 2005). Recently, the Icelandic company deCode Genetics announced that it detected a variant of a gene that increases the risk of heart attack in African-Americans by more than 250%. Nicholas Wade, *Genetic Find Stirs Debate on Race-Baced Medicine*, THE NEW YORK TIMES at A14 (November 11, 2005).

[70] In 2003 DNAPrint Genomics assisted the law-enforcement officials of Louisiana in allocating a serial killer. While the police, based on the FBI profile, was looking for a white male aged 25 to 35, the DNA Print indicated that the suspect is most likely African-American. *DNAPrint's DNA Witness Test Provided Break in the Louisiana Multi-Agency Homicide Task Force Serial Killer Case* (June 5, 2003) available at http://www.dnaprint.com/welcome/press/press_recent/2003/june_5/ (last visited January 2006); for a similar event that took place in Colorado *see DNAWitness™ Used to Guide the Investigation of the '97 rape and murder of Susannah Chase* (January 29, 2004) available at http://www.dnaprint.com/welcome/press/press_recent/2004/january_29/ (last visited January 2006); and in California: *DNA Witness Used to Guide the Investigation in Trail Side Murder Case in Concord, California* (October 14, 2003), available at http://www.dnaprint.com/welcome/press/press_recent/2003/october_14/ (last visited January 2006).

abovementioned services for a fee.[71] Private forensics is especially problematic. The U.K. Human Genetics Commission recommended that the police and other official bodies should not have access to genetic research databases so as not to deter people from taking part in research projects, which are important for the understanding of the human genome.[72] Similarly, should the public fear that the private data they entrust to these private companies for research or personal purposes may be used for a different goal than the one they agreed to, *e.g.*, for police work and records, public trust will be compromised and research may be hindered.

For the most part, private genetic databases have one of two purposes.[73] The first is clinical, providing for-a-fee service for individuals who are potentially at risk for certain genetic disorders or for individuals who desire to determine their genetic routes and origins. The other is for the purpose of conducting research for the development of future medical products and treatments.[74] In order to provide these services, pharmaceutical and biotechnology companies have recently begun to create their own private bio-repositories consisting of genetic information and tissue samples.

Genomics Collaborative, Inc., a privately-held biotechnology company established in 1998 and located in Cambridge, Massachusetts, claims to have in its possession a repository containing 500,000 tissue and DNA samples from 120,000 people from all over the world.[75] Ardais Corporation, a clinical genomics company founded in 1999, entered into agreements with several hospitals in the United States

---

[71] *See* DNAPrint Genomics' homepage at http://www.dnaprint.com/index.html (last visited January 2006).

[72] U.K. Human Genetics Commission, *supra* note 28, at 13.

[73] McEwen, *supra* note 3, at 240-242.

[74] One trend observed is the growing focus on the genetics of race. The drug BiDil, for example, is to be the first "racial drug." The drug developed by NitroMed is approved for the treatment of heart failure exclusively in the African-American population, after it was found to be unsafe for the general public. *See also*, *supra* note 69.

[75] *See* Genomics Collaborative Fact Sheet, available at: http://www.genomicsinc.com/Genomics_Collaborative_Fact_Sheets.pdf (last visited January 2006); and *also* Mark D. Uehling, *Blood, Sweat, and Tissue*, BIO-IT WORLD (March 17, 2004) at: http://www.bioitworld.com/archive/031704/blood.html (last visited January 2006).

including Duke University Medical Center in Durham and Maine Medical Center in Portland, in order to broaden and advance its library of tissue samples and information. Under these agreements Ardais receives the remains of tissue samples from surgical or other medical procedures, which are to be used for its own research and commercial purposes. The samples received by Ardais are further linked to coded information from the patient's medical records provided by the hospitals.[76] It is estimated that the Ardais biobank library – the Biomaterial and Information for Genomic Research (BIGR™) Library – contains approximately 220,000 tissue samples collected from more than 15,000 donors.[77] Ardais has commercial agreements with more than 25 pharmaceutical companies, granting them access to this biomaterial library.[78]

However, despite the magnitude of private commercial genetic repositories, and the far reaching implications they may have on personal privacy due to the highly sensitive medical and genetic information they contain, these privately held biobanks are barely regulated at the national level. The Common Rule[79] applies only to research conducted by Federal agencies or to research conducted by non-Federal agencies using Federal money; and the regulations issued under HIPAA provide only a minimum level of protection for health information.[80] First, the HIPAA regulations do not apply to all entities but only to "covered entities,"[81] namely health plans,[82] health

[76] Winickoff, *supra* note 11, at 207-217.
[77] Uehling, *supra* note 75.
[78] Ardais Corporation Announces Agreements with AstraZeneca for Access to Clinical Samples (Feb. 4, 2003), at http://www.ardais.com/news-events/press-releases.shtml (last visited January 2006).
[79] 45 C.F.R. §46.101(a). *See also supra* note 62.
[80] SOLOVE & ROTENBERG, *supra* note 50, at 210-217.
[81] 45 C.F.R. §§160.102-160.103
[82] A "health plan" is defined as "an individual or group plan that provides, or pays the costs of, medical care." 45 C.F.R. §160.103.

care clearinghouses,[83] and health care providers.[84] While medical centers, such as the ones providing tissue sample to Ardais, are classed as "covered entities" under HIPAA, it is not clear that the privately held bio-repositories themselves fall under any of these categories. Companies receiving their samples from hospitals, as does Ardais Corporation, may be considered "business associates" of health care providers, but this does not provide direct protection under the privacy rule, and the scope of protection entailed is rather vague.[85] It is unclear, for example, that such protection would apply in the event the company faces bankruptcy.[86] Furthermore, as long as the information is in a de-identified format, as is the case in most bio-repositories, the regulations do not apply to it, even if the de-identification is not permanent and can be reversed.[87]

Even if regarded as applicable to private biotech companies that are creating bio-libraries for their research and commercial purposes, the HIPAA regulations do not address several key issues, including ownership, security, and transfer of the data, which are crucial to the adequate protection of personal genetic privacy and to the autonomy of the research subjects. Thus, in the absent of sufficient Federal protections and rather than relying on free market forces and consumer power to

---

[83] A "health care clearinghouse" is defined as "a public or private entity that processes health information into various formats – either into a standard format or into specialized formats for the need of specific entities." 45 C.F.R. §160.103.

[84] A "health care provider" is defined as "…a provider of medical or health services… and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business." 45 C.F.R. §160.103.

[85] Pew Internet and American Life Project, *Exposed Online: Why the New Federal Health Privacy Regulation Doesn't Offer Much Protection to Internet Users*, 16 (November 2001) available at http://www.pewinternet.org/pdfs/PIP_HPP_HealthPriv_report.pdf (last visited January 2006).

[86] *Id. See also infra* section II.C.5.

[87] 45 C.F.R. §164.502(d)(2). If the information becomes re-identified it becomes subject to the regulations. *Id. See also* Mark A. Rothstein, *Expanding the Ethical Analysis of Biobanks*, 3 JOURNAL OF LAW, MEDICINE & ETHICS 89, 91-92 (2005).

insure the safekeeping of this sensitive data and material,[88] there is need to formulate industry-specific, self-regulated, fair information practices.[89]

C. Self-Regulation

Self-regulation[90] includes the three traditional components of government regulation – legislation, enforcement, and adjudication – only at least one of these components is carried out by the private sector; not the government.[91] There are various benefits to self-regulation.[92] First, self-regulation is considered to be quicker and easier to achieve compared to government regulation as it is less subject to political backlashes. As a result it is also cheaper.[93] Second, self-regulation is more flexible than government regulation. This is important particularly when dealing with new technologies that tend to evolve more quickly than the government operates.[94] Third, self-regulation can be designed to better fit the needs of specific industries, such as the biotechnology industry. Fourth, it is argued that self-regulation, which is developed by peers, provides better incentives to comply with. Fifth, self-regulation may be particularly useful "where the rules or adjudicatory procedures differ from the

---

[88] Consumer power may be particularly problematic because of the sensitive nature of genetics and the high transaction costs involved.

[89] *See also* SOLOVE, *supra* note 16, at 105 on the importance of fair information practices in the information age.

[90] The term "self-regulation" may have different meanings to it: "At one end of the spectrum, the term is used quite narrowly, to refer only to those instances where the government has formally delegated the power to regulate, as in the delegation of securities industry oversight to the stock exchanges. At the other end of the spectrum, the term is used when the private sector perceives the need to regulate itself for whatever reason – to respond to consumer demand, to carry out its ethical beliefs, to enhance industry reputation, or to level the market playing field – and does so. *See* Irving, *supra* note 31.

[91] Angela J. Campbell, *Self-Regulation and the Media*, 51 FEDERAL COMMUNICATIONS LAW JOURNAL 711, 714-715 (1999).

[92] *See also* Campbell, *id.*, at 715-717.

[93] Critics of self-regulation criticize this point, arguing that self-regulation simply shifts the cost of regulation from the government to the private sector, which may not be willing to commit the needed financial resources in order to obtain vigorous self-enforcement. *See* Campbell, *id.*, at 718.

[94] *See also* Llewellyn J. Gibbons, *No Regulation, Government Regulation, or Self-Regulation: Social Enforcement or Social Contracting for Governance in Cyberspace*, 6 CORNELL JOURNAL OF LAW AND PUBLIC POLICY 475, 509-510 (1997); and Gal Eschet, *FIPs and PETs for RFID: Protecting Privacy in the Web of Radio Frequency Identification*, 45 JURIMETRICS JOURNAL 301, 323 (2005).

surrounding community or the rules of the surrounding community are inapplicable," a phenomenon which is typical to the online environment.[95] As a result of these benefits self-regulation is argued to be more efficient compared to government regulation.[96] Critics of self-regulation, on the other hand, question the incentives the industry has to regulate itself and whether self-regulation in fact gives sufficient attention to the needs of the public, rather than promoting the industry's own business and economic goals.[97] Nonetheless, with proper incentives from the government as well as the market, in addition to some supervision by the government, self-regulation should be able to provide better privacy protections in the genetic realm than the existing ones, designed for the specific needs of this domain.

The purpose of establishing fair information practices, implemented directly by the industry, is to promote and protect personal privacy in bio-repositories and genetic databases and to insure coherent "best practices" among both public and private repositories, best practices which are currently lacking.[98] The key principles of fair information practices, as set out by the 1973 report of the Secretary of the United States Department of Housing, Education, and Welfare (HEW)[99] and the 1980 privacy guidelines issued by the Organization for Economic Cooperation and Development (OECD)[100] are: notice, choice, access, security, and enforcement.[101] These plus some of the more specific issues pertaining to genetic information and genetic privacy –

---

[95] Campbell, *supra* note 91, at 717.
[96] *See* Campbell, *id*., at 715-716.
[97] For these and additional criticism on self-regulation *see* Campbell, *id.*, at 717-719.
[98] The incoherent practices taken by the different companies and institutions managing bio-repositories is evident from *infra* table 1. *See also* EISMAN ET AL., *supra* note 35.
[99] Records, Computers, and the Rights of Citizens, Report of the Secretary's Advisory Committee on Automated Personal Data Systems (July 1973), available at: http://www.epic.org/privacy/hew1973report/ (last visited January 2006).
[100] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal data (1980) at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (last visited January 2006).
[101] *See* Eschet, *supra* note 94, at 324-325.

such as questions of ownership and transferability[102] – are insufficiently regulated at the present time and require further consideration.

1) Property Rights in Genetic Information

As science and technology advance, and with the growing understanding of the human genome, genetic information may reveal great amounts of highly personal sensitive information. Because of this, adequate protection for genetic information is needed to safeguard one's privacy interests, autonomy, and dignity. The question is, should the law recognize property rights to one's genetic information in order to enhance the protection granted to it, or does the right to privacy provide sufficient protection?

The famous court decision in the case of *Moore v. the Regents of the University of California*[103] did not recognize the existence of a patient's property rights to bodily parts once removed from the patient's body.[104] Moore was treated at the Medical Center of the University of California at Los Angeles for hairy-cell leukemia. In the course of treatment Moore's spleen was removed and was later used by the treating physician to establish a cell-line derived from Moore's T-lymphocytes. The cell line, which had promising research uses, was then patented by the University.[105] Moore claimed to have property interests in his removed spleen and hence also in the patented cell line.[106] The majority opinion, rejecting Moore's conversion claim, explained that granting such property interests to the individual would unnecessarily hinder medical research, and thus would harm society as a

[102] The question of transfer of sensitive medical information to insurance companies and employers is covered by the HIPPA regulations, and is forbidden under it, but the regulations do not address the question of transfer of medical and genetic data to a third party that is neither an employer nor an insurance company.
[103] *Moore v. the Regents of the University of California*, 793 P.2d 479 (Cal. 1990).
[104] *Id.*, at 134-142.
[105] *Id*.
[106] *Id*.

whole. [107] One's privacy and autonomy interests, the majority stated, can be sufficiently protected via fiduciary duty and informed consent and thus there is no need to resort to property rights that would inflict additional costs on society.[108] In contrast, in dissenting opinions, Judge Mosk argued that recognizing ownership interests in tissues "would give patients an affirmative right of participation,"[109] and Judge Brousard added that the law of conversion protects a patient's right to control the future use of his organs.[110]

Is genetic information different from body parts? Should an individual have the ability to protect her genetic information via property rights? It could be claimed that each individual DNA is unique and belongs to the person from whom it was derived, thus recognizing ownership rights in genetic information.[111] A similar claim made by Moore with regard to his spleen was rejected by the Majority opinion, concluding that a person does not have property interests in her removed body parts. It could also be argued that since the United States Patent and Trademark Office (PTO) recognized gene sequences as patentable subject matter,[112] thus granting researchers property rights over human DNA fragments,[113] there is no restriction to grant such rights to individuals. However, applying the majority's argumentation in the *Moore* case also seems to reject granting property interests in genetic information to the

---

[107] *Id.*, at 142-147.
[108] *Id.*, at 142-147.
[109] *Id.*, at 181.
[110] *Id.*, at 155.
[111] Allen, *supra* note 10, at 49-51.
[112] Patents on gene sequences are granted as long as they show "specific and substantial utility that is credible." *See* ANDREWS, MEHLMAN, & ROTHSTEIN, *supra* note 1, at 162-163.
[113] For further discussion on the patenting of genes *see* Rebecca S. Eisenberg, *Re-Examining the Role of Patens in Appropriating the Value of Gene Sequences*, 49 EMORY LAW JOURNAL 783 (2000); Michael A. Heller & Rebecca S. Eisenberg, *Can Patents Deter Innovation? The Anticommons in Biomedical Research*, 280 SCIENCE 698 (1998); and Melissa L. Sturges, *Who Should Hold Property Rights to the Human Genome? An Application of the Common Heritage of Humankind*, 13 AMERICAN UNIVERSITY INTERNATIONAL LAW REVIEW 219 (1997).

individual to whom the information pertains, a position that has been repeated in the legal literature for various reasons.[114]

For one, granting the individual property rights over genetic information could impede genetic research by increasing the transaction costs of obtaining access to genetic material and information, which is a growing part of today's medical research.[115] Secondly, it has been claimed that treating genetic information as a commodity, *i.e.*, granting property rights in the individual, disregards personhood values and interests in the self, rather than enhancing its protection.[116] Thirdly, property rights do not seem to be adequate to protect personal information, primarily because, unlike other types of property, we wish personal information to be free of alienability.[117] Privacy concerns should allow the individual to prohibit the retransfer of personal information from its holder to a third party, and be in a position to bind the new recipient with the same constraints that applied to the original holder of the information.[118] Traditional proprietary protection is therefore inadequate for protecting personal data such as genetic information.[119]

---

[114] *See* Radhika Rao, *Property, Privacy, and the Human Body*, 80 BOSTON UNIVERSITY LAW REVIEW 359 (2000) (stating that: "we should adopt the language of privacy rather than that of property when we seek to protect self-ownership without suggesting that rights in the human body can be conveyed to others and when we wish to distinguish gifts of the body to family members from sale to strangers"). *Id.*, at 434-435; and *also* Sonia M. Suter, *Disentangling Privacy from Property: Toward a Deeper Understanding of Genetic Privacy*, 72 GEORGE WASHINGTON LAW REVIEW 737 (2004); and Allen, *supra* note 10.

[115] *See Moore v. the Regents of the University of California*, *supra* note 103; and *also* Heller & Eisenberg, *supra* note 113.

[116] Suter, *supra* note 114, at 745-747; Allen, *supra* note 10, at 49-51.

[117] *See* Pamela Samuelson, *Privacy as Intellectual Property*, 52 STANFORD LAW REVIEW 1125, 1137-1138 (2000); Suter, *id.*, at 800-801.

[118] *See also* Schwartz, *supra* note 12, at 2090-2094 (advocating for a "hybrid inalienability" model that permits individuals to trade their personal information while placing limitations on its future uses, rather than viewing property rights as automatically entailing free alienability). *Id.*, at 2094-2100.

[119] Samuelson, *supra* note 117, at 1138-1139. *See also* Mark A. Lemley, *Private Property*, 52 STANFORD LAW REVIEW 1545, 1554 (arguing against intellectual property rights for personal information: "If we want privacy, we must be willing to accept the fact that there is no good 'market solution' and endorse some government regulation of the behavior of data collectors. For the reasons I have suggested, I think granting property rights in data to individuals is not a plausible solution. In particular, it is not a "free market" solution, because we cannot expect the market to allocate those billions of rights efficiently.") For a somewhat different view *see* Schwartz, *id.* at 2090-2100.

Yet, in order to achieve the same degree of protection that property law grants to personal property, the existing privacy protection for personal genetic information must be enhanced. Absent meaningful privacy protection measures and meaningful constraints on the assembly, use, and transfer of genetic information and bodily tissues, one does not have meaningful control and decisional power over her own personal genetic information and the uses made of it once in the hands of research or commercial institutions.

Put differently, if property rights in bodily tissues and genetic information are to be avoided, for moral reasons as well as for the benefit of scientific research and the common good, there is a need to strengthen the privacy protection mechanisms currently available for genetic information and genetic material. If the industry does not want to hinder its own research and scientific advancements by pushing the public into a property rights regime in genetic material, it should adopt fair information practices that would effectively safeguard the privacy and autonomy of the people whose genetic information it collects.[120] Additional aspects of genetic information collections – such as the sensitivity of the information collected, accessing it, its security, and transferability – intensify the need for fair information practices for the regulation of genetic databases and biobanks.

2) Identifiable Information

The sensitivity of genetic information has different levels and degrees. The more sensitive the information, the greater protection it requires.[121] For example, the color of one's eyes falls under the definition of personal genetic information,[122] but it

[120] *See also* Campbell, *supra* note 91, at 715 (noting that "often times, an industry will engage in self-regulation in an attempt to stave off government regulation").
[121] Gostin, *supra* note 24, at 519-521; U.K. Human Genetics Commission, *supra* note 28, at 4-6, 10-11.
[122] The U.K. Human Genetics Commission defines personal genetic information as: "any information about the genetic make-up of an identifiable person, whether it comes from DNA testing or from

is not as sensitive as genetic information of a medical nature such as that regarding a predisposition for certain diseases like breast cancer or Alzheimer's.[123] While the latter – if learned – may be the cause for insurance and even employment discrimination, the former is unlikely to cause the same effect; hence the difference in sensitivity is evident.

Another important attribute to the sensitivity of the information depends on whether the information may be linked to an identifiable person. The European Union Directive on Data protection defines "personal data" as: "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[124] Similarly, the OECD privacy guidelines define personal data as "any information relating to an identified or identifiable individual (data subject)."[125]

Because genetic information has various degrees of sensitivity, based largely on whether or not the information is identifiable, it is useful to distinguish between genetic information collected for clinical purposes and that collected for research purposes. In the clinical context, such as genetic testing, the likelihood that the genetic information will be easily identifiable is higher than in the research context. Genetic information collected for the purpose of clinical tests will usually be directly linked to additional identifiable information such as name, address, birth date, diagnosis, and

---

any other source (including the details of a person's family history)." U.K. Human Genetics Commission, *supra* note 28, at 5.

[123] *Id.*, at 4-5.

[124] The Data protection Directive of 1995, article 2.

[125] *See* OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal data (1980), *supra* note 100.

family history in order to better diagnose, locate, and provide proper treatment to the patient.[126]

On the other hand, if the genetic information is being collected primarily for research purposes then it will usually not be directly linked to any identifiable data, and therefore, theoretically at least, will pose a lesser risk to the privacy of the individual.[127] Nonetheless, it is not impossible to link the information to a specific person if enough DNA sequences are available, due to the "unique quality" of the DNA.[128] Moreover, often times the option to link genetic information, obtained for research purposes, to an identifiable person will be retained by the research institutions, so as to have the ability to contact the person in the event a genetic disorder is discovered, or in case further medical information is needed.[129] Linkage to medical records may also reveal indirect identifiable information as well as certain demographic data.[130] Hence, privacy protection measures must also be taken with regard to information that is not directly identifiable, but has the potential to be identified.

The HIPAA regulations, previously mentioned, apply only to identifiable information.[131]As a result, a considerable amount of genetic data available in private bio-repositories and which is de-identified, is not subject in its de-identified form to the HIPAA regulations and their privacy requirements.[132] A number of private bio-repositories have implemented HIPPA requirements, despite claiming that they are not obliged to do so, and it has been found that others even implemented more

[126] McEwen, *supra* note 3, at 240-242.
[127] McEwen, *id.*, at 240-242.
[128] *See* Murray, *supra* note 19, at 63; Gostin, *supra* note 24, at 504.
[129] The U.K. Biobank, for example, gives the participants the option to choose whether or not they want to be informed in such event. *See* U.K. Human Genetics Commission, *supra* note 28, at 17.
[130] Rothstein, *supra* note 87, at 90.
[131] 45 C.F.R. §164.502(d)(2).
[132] It should be noted that once the information is re-identified, it becomes subject to the regulations. *Id*.

stringent practices than those required under HIPPA.[133] This may indicate a need for more regulation than currently available, regulation that may be achieved via formulation of fair information practices. Adopting clear guidelines is also likely to enhance public trust and the willingness to take part in research projects.[134]

3) Access

As part of their services, commercial bio-repositories frequently offer pharmaceutical companies and research institutions access to their private bio-libraries. This is necessary to the advancement of research and might remind some of the traditional collaborative science, or be perceived as a new form of open-source access to biotechnology.[135] Nonetheless, this also requires extra caution in order to protect the personal privacy of the data subjects.

It is important to have guidelines as to who may have access, and to what types of information. Third parties that are given permission to research the information stored in biobanks or genetic databases should only have access to unidentifiable information that cannot be re-identified without the prior consent of the individual.

Specific guidelines as to when encrypted data may be de-encrypted and by whom, should be formed. All employees with access to sensitive data must adhere to confidentiality agreements or policies that are to be strictly enforced.[136] Only a restricted number of personnel should have access to identifiable information and to the linking key between the anonymized genetic information and the person to whom it pertains. There should also be limitations set on the uses of this information, so as

[133] EISMAN ET AL., *supra* note 35, at 130-132.
[134] *See also* Rothstein, *supra* note 87, at 94-95.
[135] *See also* David W. Opderbeck, *The Penguin's Genome, or Coase and Open Source Biotechnology*, 18 HARVARD JOURNAL OF LAW & TECHNOLOGY 167 (Fall 2004).
[136] U.K. Human Genetics Commission, *supra* note 28, at 18.

to ensure that the information is being used for the research purposes agreed to by the research subject rather than unwarranted uses that may lead to, for instance, employment or insurance discrimination.

4) Security

In addition, and of no less importance, genetic databanks and bio-repositories need be secured from unauthorized access (both in the physical as well as the virtual worlds). As table 1 indicates, currently there is no single uniform standard for the protection of sensitive genetic information. For instance, while some companies choose to encrypt the information they collect, others do not, and even encrypted information is potentially exposed to decoding.[137]

The existing variation in bio-repositories and lack of uniform standards not only impede research by making it more difficult to compare results from specimens taken from different banks,[138] but also undermine the privacy interests of the research subjects since it is more difficult and costly for them to find out what measures are taken by each institute, and which measures would provide adequate privacy protection. In other words, the diversity in security measures taken by different institutions imposes additional transaction costs on data subjects who care for their privacy thus making it more difficult for the market to regulate itself towards implementing stronger privacy protections.[139]

[137] *See also* the criticism voiced on the encryption mechanism adopted by the Icelandic Health Sector Database Act. *Infra* note 212 and the accompanying text.
[138] ELISA EISEMAN ET AL., *supra* note 32; Mark D. Uehling, *Study: Federal Banks are Lagging*, BIO-IT, available at http://www.bio-itworld.com/archive/031704/blood_sidebar_4640.html (last visited January 2006).
[139] Under a market approach it is assumed that consumers would prefer to do business with those companies that better protect their privacy. *See also* Eschet, *supra* note 94, at 321.

Table 1: Tissue Repositories Security Measures

	# of human specimens	searchable at secure online site	Access to quality control data	Encryption data identifying donor	Overseen by ethics advisory board	Requires SOPs[140] for tissue collection
Armed Forces Institute of Pathology	92 million			X		
Genomics Collaborative	500,000	partial	X		X	X
Ardais Corp.	220,000	X	X	X	X	X
National Cancer Institute's Cooperative Human Tissue Network	107,000	partial	partial	X	X	X
Mayo Clinic Prostate Specialized Program of Research Excellence (SPORE)	3,000		X	X		X
University of Pittsburgh Health Sciences Tissue Bank	1,100	X	X	X	X	X

Source: bio-itworld.com at http://www.bio-itworld.com/archive/031704/blood_sidebar_4641.html

Appropriate security measures should not only restrict external access to the information by hackers, but also the number of interior personnel that have access to personal information, particularly identifiable or potentially identifiable information.[141] Data retrieved from the linkage of personal information and databases and data that has greater potential of being identifiable should be subject to the highest form of security measures, including data encryption, and only a restricted number of personnel should have access to it on a need-to-know basis.

5) Transferability

For commercial biotech companies, their databases, containing the genetic information of individuals, are one of their most valuable assets. One major concern is that absent proper restrictions, companies would treat genetic databases and biobanks as they would treat any other commercial asset, despite their sensitive nature. For

[140] Standard Operating Procedures.
[141] EISMAN ET AL., *supra* note 35, at 121-126, 135.

instance, the companies might sell their databases in case of financial difficulty, or simply for the sake of making profit, just as they might with any other valuable asset they possess.[142]

The issue of genetic databases as a commercial asset raises several difficult problems. First, genetic databases contain highly sensitive information which, in some cases, can be directly linked to specific individuals whether they chose to be part of the database (as in the case of voluntary genetic testing) or not (as in the case of forensic databases). Second, it is not clear that the company collecting the information is indeed the owner of that information,[143] and thus whether it is free to sell or transfer said information at its will. It has been suggested by scholars that the holders of medical data should be considered as merely "trustees," not owners, of the data, a position that places greater restrictions and responsibilities over the authorized uses of the data and puts limitations on its future disclosure.[144] At the very least, the individuals to whom the information pertains should be able to place limitation on future uses of their genetic information in order to maintain their autonomy interests.[145]

If a company decides to sell its genetic databases to another entity, the privacy of this sensitive, potentially identifiable information is jeopardized. A similar concern exists with regard to personal user information collected, for example, by online

[142] For additional examples of the commodification of personal information in the technology age *see* Schwartz, *supra* note 12, at 2060-2069, 2127-2128. For a more general discussion of this trend *see* THE COMMODIFICATION OF INFORMATION (Niva Elkin-Koren & Neil W. Netanel eds., 2002).
[143] *See* generally SOLOVE, *supra* note 16, at 78-79.
[144] For more on holders of health information as "trustees" *see* Schwartz, *supra* note 15, at 57-59; and *also* Winickoff & Winickoff, *supra* note 35, at 1182-1183 (advocating for a charitable trust model for genomic biobanks in order to, among other things, insure "longevity" and prevent the transfer of genetic material without the prior informed consent of the tissue donor). *See also* SOLOVE, *id.*, at 102-104 (suggesting that companies that collect and store personal information stand in a fiduciary relationship with the individuals to whom the information pertains).
[145] *See* Schwartz, *supra* note 12, at 2094-2100.

retailers.[146] This information, which includes the purchasing habits of consumers, billing information, and similar consumer profiles, is subject to ownership transfer in the event of bankruptcy or other financial problems faced by the companies.[147] But, while the privacy policies of such dot-com companies often address the question of transfer of sensitive information to third parties,[148] DNAPrint Genomics, for example, which provides an array of genetic services from paternity rests to private forensics,[149] fails to specifically address this scenario in its Code of Ethics.[150] In the absence of a Federal law prohibiting such sale of personal genetic information and in view of previous court decisions allowing the transfer of personal information from one entity to another,[151] the sale or transfer of genetic information to a third party seems like a realistic probability.

In fact, at the end of March 2005 Ardais Corporation and Cytomyx Holdings plc, a life science company based in the United Kingdom, announced their newly formed collaboration. Under the Collaboration, Cytomyx will acquire and gain control over the Ardais biorepository containing over 130,000 samples.[152] While the press release announcing the collaboration and transfer of ownership over the Ardais biorepository assured that all former business customers would continue to have access to and use the samples in the biobank, nothing was said with regard to the

---

[146] *See also* SOLOVE, *supra* note 16, at 83.
[147] *See In re Toysmart.com, LLC* (Bankr. D. Mass. 2000) in which the court concluded that Toysmart could sell its consumers' personal information database despite its privacy policy which stated that "personal information voluntarily submitted by visitors to our site, such as name, address, billing information and shopping preferences, is *never* shared with a third party" (emphasis added).
[148] *See* for example the privacy policy of Amazon.com that specifically stipulates that "…in the unlikely event that Amazon.com, Inc., or substantially all of its assets are acquired, customer information will of course be one of the transferred asset." *See* http://www.amazon.com/exec/obidos/tg/browse/-/468496/102-0508312-4688103 (last visited January 2006).
[149] *See supra* note 71 and the accompanying text.
[150] *See* DNAPrint Genomics, Code of Business Conduct and Ethics, available at http://www.dnaprint.com/2003/corporate/ethics (last visited January 2006).
[151] *See In re Toysmart.com*, *supra* note 147.
[152] Ardais and Cytomyx Announce Translational Medicine Collaboration (March 30, 2005), at http://www.ardais.com/news-events/press-releases.shtml (last visited January 2006).

safekeeping of the privacy interests of those whose medical and genetic data have just been transferred to a new entity, located outside of the United States.[153]

Ironically, it is likely that the personal information now controlled by a British company is actually better protected than before, because the European Union generally provides broader privacy protections than the United States.[154] However, absent legal restrictions on the transfer of genetic information abroad, future collaborations may end with transfer of genetic information to countries that offer a lesser level of privacy protection compared to that available in the United States, or even no privacy protection at all; a situation that should not be permitted.

It may be argued that transfer of ownership in genetic databases and biobanks does not necessarily affect the privacy interests of individuals, particularly if the information transferred in coded, or that the market powers are sufficient to safeguard privacy interests, but this is not reassuring. First, changes in ownership make it more difficult for the data subjects to control the uses made with the information and increases the possibility that the information may be used for purposes others than the ones agreed for. Second and as previously explained, pure market forces are unlikely to give adequate remedy due to market failure in the form of high transaction costs that prevent consumers from preferring those companies that implement strong privacy protections.[155] Moreover, in the computerized world in which we live, personalized data can easily and cheaply be transmitted from one country to the other. Absent any meaningful regulation this could further undermine personal privacy. This scenario is especially plausible when the data is being controlled by a private, commercial company that primarily seeks to maximize its profits. Lastly, the same type of alienability argumentation that sees personal information as different from

[153] *See id.*
[154] *See infra* note 157 and the accompanying text.
[155] *See also supra* note 139 and the accompanying text.

other types of property,[156] applies here. If personal information should be free of alienability, then the data subjects should be able to prohibit the transfer of information pertaining to them to third parties.

For similar reasons and in order to protect privacy interests, the European Union permitsthe transfer of personal information only to states that grant sufficient privacy protection measures;[157] and the Icelandic parliament, which was willing to provide access to all of its national's medical records to a private company, insisted that the company be located in Iceland, and that the data not leave the country.[158] However, such limitations are largely absent in the United States, especially when dealing with private companies. As a result, research subjects are lacking control and further assurances over their personal information and its uses. Hence, limitations on the transfer of genetic information including with respect to its location, the entity receiving it, and its future usages, are required.[159]

In sum, there is need for more scrutiny to be applied not just towards Federal or national public repositories, but also towards private commercial entities. This could be achieved through the establishment of fair information practices. At the same time, more supervision should be directed at collaboration initiatives between the state and private commercial companies and the flow of information from the public to the private sector. The following section will analyze the privacy threats posed by these new collaborations using the Icelandic Health Sector Database as a case study.

---

[156] *See supra* note 117.
[157] *See* the European Data Protection Directive of 1995, article 25.
[158] Act on a Health Sector Database, no. 139/1998 (passed on Dec. 17, 1998) (Hereinafter: the HSD Act), article 10. English version available at http://www.informatica-juridica.com/anexos/anexo610.asp (last visited January 2006).
[159] *See also* FRANCIS FUKUYAMA, OUR POSTHUMAN FUTURE, CONSEQUENCES OF THE BIOTECHNOLOGY REVOLUTION, chapter 10 *The Political Control of Biotechnology*, 181-194 (2002) (Stressing the need for regulation, particularly international regulation, to control biotechnological advances).

III. PRIVATE – PUBLIC PARTNERSHIPS IN THE GENETIC ERA

A. The Icelandic Health Sector Database

There is an extensive debate about whether private or governmental control over personal data is more intrusive and which requires more precautions. The traditional American thought is more wary of the government;[160] while its European counterparts have more faith in government and less in industry. The former, as a result, places greater restrictions on the government than on private industry.[161] However, as recently suggested by legal scholars Michael Birnhack and Niva Elkin-Koren, we must now also be conscious of a new player, a partnership between the two, referred by them as the "Invisible Handshake" between the government and the private industry.[162]

The Icelandic Health Sector Database Act, under which the Icelandic government granted a private, for-profit, American company access to all of Iceland's

---

[160] *See*, for example, Chris Jay Hoofnagle, *Big Brother's Little Helpers: How ChoicePoint and other Commercial Data Brokers Collect and Package Your Data for Law Enforcement,* 29 NORTH CAROLINA JOURNAL OF INTERNATIONAL LAW AND COMMERCIAL REGULATION 595, 629-630 (2004) (Stating: "Our Nation also has a deep suspicion of government action and motives, while maintaining trust in the action of the private sector. … Libertarians and conservatives…have argued that government collection, use, and disclosure of information presents more risk commercial collection because the government has the power to arrest, imprison, and even to execute citizens. Commercial entities, although they hold our mortgages and often control our employment, arguably present less risk to our autonomy.").

[161] *See also* Joel R. Reidenberg, *E-Commerce and Trans-Atlantic Privacy*, 38 HOUSTON LAW REVIEW 717, 730-731 (2001) (stating that: "…the United States has, in recent years, left the protection of privacy to markets rather than the law. In contrast, Europe treats privacy as a political imperative anchored in fundamental human rights. … This vision of governance generally regards the state as the necessary player to frame the social community in which individuals develop and in which information practices must serve individual identity. … Indeed, citizens trust government more than the private sector with personal information.").

[162] Michael D. Birnhack & Niva Elkin-Koren, *The Invisible Handshake: The Reemergence of the State in the Digital Environment*, 8 VIRGINIA JOURNAL OF LAW & TECHNOLOGY 6 (Summer 2003) stating that: "Whether the big brother we distrust is government and its agencies, or multinational corporations the emerging collaboration between the two in the online environment produces the ultimate threat." *Id*. at 1. (Birnhack & Elkin-Koren point to the rise of the Invisible Handshake between the government and the private industry in the Information Technology realm, primarily the growing use by the government of the tools developed by the industry for its own commercial and legal needs). *See also* Hoofnagle, *supra* note 160, at 630 (arguing that the "distinction between the risks of government and commercial privacy risk is no longer tenable. Commercial actors provide personal information to the government in a number of contexts, and often with astonishing alacrity"). In the genetic context the information flow between the private and public sectors occurs mainly in the direction of the private sector from the public one, in return for financial compensation. *See also* Petersen, *supra* note 9 and the accompanying text.

medical files, along with a license to compile them all into one digital database that is linked to genetic information, is a good (some would say alarming) example of the new relationship and collaboration between the private and public sectors in the context of genetic privacy.

1) The Icelandic Health Sector Database Act

The Icelandic Act on a Health Sector Database[163] (the "HSD Act"), enacted in December 1998, attracted much attention and criticism since it was first introduced in 1997. The Act establishes the Icelandic Health Sector Database on an opt-out basis,[164] and aims to, as stated in the Act itself, "authorize the creation and operation of a centralized database of non-personally identifiable health data with the aim of increasing knowledge in order to improve health and health services."[165] The creation of the database and the genealogical research it would allow was believed to be especially beneficial. In this regard, the Icelandic population was viewed as a particularly good case study because of its genetically homogenous nature, which was believed to make it relatively easier to spot genetic variations associated with diseases.[166]

The database, including all health information it contains, is to be managed exclusively by a private commercial American company, deCode Genetics Inc. ("deCode"). In fact, the Health Sector Database Bill was drafted on the basis of a

[163] The HSD Act, *supra* note 158.
[164] The HSD Act, *id*, article 8.
[165] The HSD Act, *id.*, article 1.
[166] The validity of this argument is somewhat questionable because humans share 99.9% of the genome and most genotype variation is found within races or ethnic groups, not between them. *See also* Henry T. Greely, *Iceland's Plan for Genomics Research: Facts and Implications*, 40 JURIMETRICS JOURNAL 153, 159-160 (Winter 2000) (listing six additional benefits for conducting this type of research in Iceland: 1) Iceland's relatively small size; 2) the general support granted by the Icelandic people to medical research; 3) an organized national health coverage that collected information and tissue samples since the first half of the 20th century; 4) the obsession the Icelandic people have with genealogy; 5) all Icelandic people experience relatively similar environment; and 6) the existence of a political will to allow large scale genetic research).

proposal made by deCode itself.[167] The Bill was criticized on numerous accounts including that it lacked provisions for obtaining informed consent of individuals whose information was included in the database, undermined scientific freedom, restrained competition, eroded the doctor-patient confidential relationship, and invaded the people's right to privacy.[168] Nonetheless, in December 1998, shortly after first introduced, the Bill was enacted by the Icelandic parliament, the Althingi.

DeCode was granted a 12-year license[169] to construct an electronic database for all health records available in the Icelandic national health care system, namely, the health records of approximately 270,000 citizens, as well as records dating back to the first half of the 20th century.[170] The subjects of the database include the deceased, children, and incompetent individuals, all of whom cannot legally provide informed consent to this move. This electronic database was designed to contain extensive medical information including: records on the individuals' health, their medical treatments, lifestyles, social circumstances, employment, and family.[171] DeCode was further authorized to link this health information to two additional databases: Iceland's genealogy database and to other genetic data collected from volunteers from within the Icelandic population.[172]

---

[167] Ragnar Aðalsteinsson, *The Constitutionality of the Icelandic Act on a Health Sector Database*, in SOCIETY AND GENETIC INFORMATION: CODES AND LAWS IN THE GENETIC ERA, 203, 203-204 (Judit Sándor ed., 2003). Due to numerous criticisms the Bill was substantially amended from the original draft. One of the new provisions added was the opt-out option. *See id*. For a list of additional changes made from the first to the second draft of the HSD Act *see* Greely, *id.*, at 170-171.

[168] Aðalsteinsson, *id.*, at 204-205.

[169] The HSD Act, *supra* note 158, article 5(9).

[170] Greely, *supra* note 166, at 159-161.

[171] *Ragnhildur Guðmundsdóttir v. The State of Iceland*, No. 151/2003 (November 27, 2003), part IV. English version available at http://www.mannvernd.is/english/lawsuits/Icelandic_Supreme_Court_Verdict_151_2003.pdf (last visited January 2006).

[172] *See* The HSD Act, *supra* note 158, article 10; and *also* Winickoff, *supra* note 11; and Kaiser, *supra* note 7. According to the Biobanks Act of 2001, any patient whose biological sample has been taken is presumed to have consented to the storage of the sample in a biobank for the purpose of scientific research, unless the patient explicitly indicates otherwise. *See* Aðalsteinsson, *supra* note 167, at 208-209.

Put another way, the HSD Act granted deCode, a private commercial company, presumed consent (or "blanket consent"[173]) to collect the medical records of the entirety of the Icelandic population,[174] compile them in one electronic database, and combine this data with available genetic information, unless specifically indicated otherwise by each individual in a pre-defined six-month window.[175]

2) Privacy Protection under the HSD Act

The HSD Act raises many concerns including the commercialization of personal medical data, and intrusion upon medical privacy.[176] The fact that the government, which was entrusted with this sensitive information for generations, was willing to transfer the people's medical records to a private for-profit company without obtaining explicit individual consent for this move is very troubling. This is so especially since private commercial companies are likely to have different goals at heart: while the government is expected to act primarily for the benefit of the public good, a for-profit company is likely to act on its own economic interests, even when such interests conflict with the public welfare.[177] Furthermore, the inadequate protection granted in the Act to that information and to the privacy interests of the population adds insult to injury.

---

[173] George J. Annas, *Rules for Research on Human Genetic Variation – Lessons from Iceland*, 342(24) THE NEW ENGLAND JOURNAL OF MEDICINE 1830 (June 15, 2000); Jeffrey R. Gulcher & Kári Stefánsson, *The Icelandic Healthcare Database and Informed Consent*, 342(24) THE NEW ENGLAND JOURNAL OF MEDICINE 1827 (June 15, 2000).

[174] This implied priori consent to transfer medical information to the HSD database is acceptable if the information transferred is unidentified, and cannot be linked back to a specific person. This issue was central to the Iceland Supreme Court decision in *Ragnhildur Guðmundsdóttir v. The State of Iceland*, *supra* note 171.

[175] The HSD Act provided a six-month grace period beginning with the passage of the Act, in which people could choose to opt-out of the project. The HSD Act, *supra* note 158, article 8. *See also infra* section III.A.3.

[176] Greely raises five main concerns stemming from the HSD Act: connection to a for-profit firm; lack of affirmative informed consent; privacy; exclusive control over the database; and the financial terms of the agreement. *See* Greely, *supra* note 166, at 176-191.

[177] For a somewhat different view *see* Greely, *supra* note 166, at 176-178 (claiming that there is no clear answer whether the government or non-profit institutions, such as universities, are better suited to operate this type of databases).

The main benefit of this colossal database, it was argued, was to boost the country's economy.[178] Some of the economic benefits emphasized were that the project would bring back Icelandic scientists who left the country, and that it would jump-start an Icelandic biotech industry.[179] However, whether or not the Icelandic parliament and the Icelandic people actually made a good deal is highly questionable.[180] The country could not meet the expense of establishing such a comprehensive database and therefore resorted to a commercial company to do so. But because of this, should the database yield the potential value hoped for, the Icelandic government's share of the profits will be surprisingly small.[181] The justification for the transfer of control over the medical records from medical personnel to administrative boards was that the medical records are not subject to property rights, but are rather a national resource.[182] However, even if the data is a national resource it is not clear why one private (American) company – rather than Icelandic institutions and companies, the government, and the Icelandic people themselves – should be the primary beneficiary.

Beyond the actual transfer of sensitive information from the government's holding to a private, for-profit company without explicit consent, which is problematic on its own, the HSD Act does not take sufficient measures to safeguard the information stored and the privacy interests that accompany it. The Act does not disregard the need for safeguarding privacy; it purports to take several measures aimed to protect the privacy interests of the Icelandic citizens. Health information and

---

[178] *See* Aðalsteinsson, *supra* note 167, at 205; and *also* Kaiser, *supra* note 7, at 1159.
[179] *Id.*
[180] *See* Greely, *supra* note 166, at 173 (stating that: "the licensee's financial obligations, as stipulated by the legislation, are not extensive. … The Act does not provide Iceland with any royalty or other share of the licensee's profits, nor does it require the provision of free drugs to Iceland that had been part of deCode's agreement with Roche."). Likewise, granting deCode an exclusive license for a period of 12 years may in fact impede other Icelandic research projects by denying access to the information contained in the database. *Id*. at 187; and *also* Annas, *supra* note 173.
[181] Greely, *id.*, at 187-191.
[182] Aðalsteinsson, *supra* note 167, at 206.

personal identification information is coded prior to its entry to the database;[183] in addition, personal identification data undergoes one-way coding that, as promised by the Act, cannot be traced by means of a decoding key.[184] The process is overseen by two governmentally-appointed bodies: the Data Protection Committee,[185] and the Committee on the Creation and Operation of a Health Service Database,[186] which are responsible for monitoring the recording and handling of the information and making sure that the data is adequately protected and that the privacy interests of the population are kept.

But these provisions, it seems, are far from sufficient to safeguard the privacy of the Icelandic population. One-way coding of personally identifiable information, for instance, is not plausible if the medical records are to be linked to genealogical data. The reason being that in order to make this link, someone – either deCode or one of the governmental committees – will need to have the decoding key, thus undermining the anonymity of the participants.[187] Moreover, if sufficient DNA sequence data is stored in the genealogical database, it is theoretically possible to identify the individual whose sequence it is, even if her name or other identifiable information is removed.[188]

The HSD Act further grants deCode the authorization to use the medical information stored in the database for its "financial profit" as long as the provisions of the Act and of the license are followed,[189] or for the research purposes of its

[183] The HSD Act, *supra* note 158, article 7.
[184] The HSD Act, *id.*, article 7. "One-way coding" is defined by the HSD Act as "the transformation of words or series of digits into an incomprehensible series of symbols which cannot be traced by means of a decoding key." The HSD Act, article 2.
[185] The HSD Act, *supra* note 158, article 12.
[186] The HSD Act, *id.*, articles 10, 12.
[187] *See* Greely, *supra* note 166, at 183-184.
[188] *See* Murray, *supra* note 19, at 63; Gostin, *supra* note 24, at 504.
[189] "The licensee is authorized during the period of the license to use the data on the database for purposes of financial profit, under the conditions laid down in this legislation and the license." The HSD Act, *supra* note 158, article 10.

licensees.[190] Drug companies may also have access to the database for a fee, and academic researchers working on "non-commercial projects" would be able to access the information at no cost.[191] The Act does not require deCode to receive informed consent from individuals in the database for specific research projects, but rather leaves the possible uses of the information unspecified,[192] effectively making it impossible for the participants in the project to have control over the current and future uses of their own medical and genetic information.[193]

3) Opting Out of the Health Sector Database

An Icelandic citizen who does not wish to be included in the national healthcare database must actively opt-out of the project.[194] The people of Iceland were given a limited, pre-defined transitional period of six months after the passage of the HSD Act and prior to the entry of medical data into the Health Sector Database to do so.[195] As a result, only about 7%-10% of the Icelandic population opted-out of the project.[196] This low percentage might be indicative of overwhelming support for the HSD Act and the Health Sector Database established under it, but it is more likely the result of the structure chosen in the form of an opt-out process, advocated by deCode, rather than an opt-in system.[197] If, in fact, the Health Sector Database enjoys such overwhelming support by the public, there should be no reason to object to an opt-in

[190] Winickoff, *supra* note 11, at 202.
[191] Kaiser, *supra* note 7, at 1159.
[192] The HSD Act, *supra* note 158, article 10.
[193] Winickoff, *supra* note 11, at 202.
[194] The HSD Act, *supra* note 158, article 8.
[195] Greely, *supra* note 166, at 172.
[196] Kaiser, *supra* note 7, at 1159; Gulcher & Stefánsson, *supra* note 173.
[197] *See also* Jeff Sovern, *Opting In, Opting Out, or No Opting At All: The Fight for Control of Personal Information*, 74 WASHINGTON LAW REVIEW, 1033 (1999) (listing the benefits of an opt-in system compared to an opt-out system).

regime, which will more accurately represent the consent of the people and safeguard their autonomy and control over the information collected.[198]

Individuals who did not opt-out within the provided "grace period" can, according to the Act, request "at any time, that either all of their existing or future medical information not be entered into the database or that specific information not be entered."[199] However, the Act does not provide for deletion of information already entered into the database, only for preventing the entry of future information.[200]

The HSD Act is also silent with regard to data collected on the legally incompetent, including children and the mentally disabled. Even though children's privacy protection has often been regarded as requiring more rigorous regulations compared to that of adults,[201] the HSD Act chose not to address this segment of the population that would be included in the Database. The guardians of the incompetent or the parents of children under 18 years of age may opt-out of the project on their behalf; in addition, once a child reaches the age of 18 she may independently opt-out of the project. But just as the adults who did not opt-out in the initial six-month grace period, this act of opting-out once reaching legal adulthood concerns only future data that might be entered into the database. Data that has already been stored in the database will not be removed or deleted simply because an individual opts out upon turning 18, even though she could not do so herself beforehand.[202]

---

[198] *See also* Greely, *supra* note 166, at 180-181; and SOLOVE, *supra* note 16, at 105-106.
[199] The HSD Act, *supra* note 158, article 8.
[200] *See* Greely, *supra* note 166, at 178-179; and *also* Winickoff, *supra* note 11, at 203; Annas, *supra* note 173. Both Winickoff and Annas interpret the Act as making such removal of already existing data in database, impossible.
[201] *See*, for example, the Child Online Protection Act of 1998 (COPA) and the Child Pornography Prevention Act of 1996 (CPPA), both of which provide enhanced privacy protection for children in the online environment.
[202] Aðalsteinsson, *supra* note 167, at 206-207. However, deCode and the Medical Association of Iceland issued a joint statement in which they promised to erase already existing data from the database at a patient's request to opt-out. Aðalsteinsson, *id*.

In addition, the HSD Act does not directly address the rights of the deceased pertaining to their health information, or put differently, the rights of the relatives to opt-out on behalf of the deceased and to refuse the transfer of the deceased's health information into the database. The latter issue was subject to a legal suit brought before the Icelandic Supreme Court.[203] The plaintiff, a young woman who asked to prevent the transfer of her deceased father's medical records into the Health Sector Database, brought suit upon the refusal to do so by the Medical Director of Health of Iceland.[204] The refusal of the Medical Director of Health was not based only on the fact that the HSD Act does not directly address this issue, but also, and primarily, on the commentary attached to the bill that indicated that the Act was never intended to enable people to prevent the transfer of information of their deceased relatives.[205]

Although according to Icelandic law, the personal rights of individuals lapse on their death unless otherwise stipulated by law,[206] the Supreme Court recognized that information regarding her father's genetic history and records, may apply also to the appellant herself.[207] The fact that genetic information may reveal medical information not only pertaining to the subject herself but also to relatives was used to argue that genetic information is different and more intrusive than other forms of medical information.[208] The Supreme Court hence accepted the appellant's argument that her constitutional right to privacy[209] grants her interest in preventing the transfer of her deceased father's medical information to the Health Sector Database.[210]

[203] *Ragnhildur Guðmundsdóttir v. The State of Iceland*, *supra* note 171.
[204] *Id.*, part I.
[205] *Id.*, part I; Aðalsteinsson, *supra* note 167, at 207.
[206] *Ragnhildur Guðmundsdóttir v. The State of Iceland, id.*, part II.
[207] *Id.*, part II.
[208] *See also supra* note 19 and the accompanying text.
[209] The right to privacy is recognized under Paragraph 1 of Article 71 of the Icelandic Constitution.
[210] *Ragnhildur Guðmundsdóttir v. The State of Iceland*, *supra* note 171, part II.

In its analysis of the HSD Act, the Icelandic Supreme Court found additional flaws with the Act and its protection of personal privacy; concluding that the one-way coding mechanism established by the HSD Act[211] is insufficient for protecting individuals' privacy. The Supreme Court's reasoning was two-fold: first, because the Act provides no specific guidance as to what type of information must be encrypted in this manner; and second, because the license seems to imply that after deletion of the name and address of a person, only her identification number needs be encrypted.[212] This, according to the Icelandic Supreme Court's opinion, does not adequately protect one's privacy interests.

The Icelandic experience described above provides further support for the need to establish and implement fair information practices targeting the accumulation of personal genetic information, and the usage and storage of this data. It also demonstrates both the risks and benefits stemming from unrestricted flow of information between public and private entities, as is further discussed in the following section.

B. Risks and Benefits

To be certain, there are valuable aspects of such collaboration between public and private entities. First, if governments hold vast amount of useful medical and genetic data, such as the Icelandic medical records[213] or the American National Pathology Repository,[214] but do not have the resources, the technology, the capacity, or the will to take full scientific advantage of it, while private entities have the

[211] *See supra* note 184.
[212] *Ragnhildur Guðmundsdóttir v. The State of Iceland*, *supra* note 171, part IV.
[213] *See supra* note 170 and the accompanying text.
[214] *See supra* note 45 and the accompanying text.

aptitude but not the data,[215] then the need for collaboration between the two is evident and will benefit science and society.

Second, private companies that collaborate with public institutions may be subject to stricter standards and greater public scrutiny compared to private entities acting on their own, thus better safeguarding privacy concerns. For instance, in contrast to the United States where there are no real restrictions on the transfer of genetic information kept in private bio-repositories,[216] the Icelandic Health Sector Database Act forbids the transport of the database outside of Iceland, and all of the information contained in the database is to be processed in Iceland alone.[217] It is unlikely that such a broad limitation on the transfer of information would have been applicable if it had not been for the involvement of the government in providing the data to the Health Sector Database.

Still, these partnerships hold many potential risks to the privacy and autonomy of individuals. First, such partnerships give private companies with commercial, profit-driven goals access to an immense amount of personal information that the government has been entrusted with. It is not clear that individuals would agree to contribute their tissue samples and genetic and medical information to private, for-profit companies without proper compensation. Hence, such transfers of data must be authorized by individuals in the form of an active informed consent.

Second, unless individuals specifically agree to the transfer of information from one entity to another, collaborations between public and private entities that involve the transfer of DNA samples and medical information undermine the autonomy and control of the research subjects. Thirdly, if one views either one of the two collaborators – either the private sector or the public sector – as posing a greater

[215] *See also* Petersen, *supra* note 9 and the accompanying text.
[216] *See supra* section II.C.5
[217] The HSD Act, *supra* note 158, article 10.

risk to her privacy interest compared to the other, then the transfer of information from one sector to the other intensifies this risk in the eyes of the individual. Lastly, and perhaps most importantly, commercial companies are likely to have a different set of priorities than those of governmental or non-profit organizations, and hence may be less fit to be the sole keepers of vast amounts of sensitive, personal information, especially if easily linked to other types of personal information.

In order to address these concerns, the transfer of information from one entity to another, in all sectors, must be thoughtfully regulated and practiced, and the explicit consent of the participants must be obtained. Moreover, it would be useful to adopt a trustee model for keepers of genetic information and samples, particularly when dealing with privately owned repositories, in order to limit potential misuses. The U.K. Biobank, which has internalized much of the criticism voiced on the Icelandic Health Sector Database, rejected the commercial model adopted by Iceland, and managed to structure a more data-subject friendly approach based on a governmental-charitable structure.

C. Lessons from Iceland: The U.K. Model

Aiming to be the largest population database in the world with human samples initially collected from 500,000 volunteers, the U.K. Biobank is to be launched in early 2006.[218] It will consist of a collection of blood and urine samples, information regarding height, weight, and blood pressure, and additional information collected via a questionnaire form from volunteers aged 40 to 69, and will follow the health of the

[218] *See* http://www.ukbiobank.ac.uk/about.php (last visited January 2006).

volunteers for long periods of up to thirty years.[219] The information is further intended to be linked to each data-subject's medical records.[220]

The purpose of the project, as indicated by its founders, is to provide a "unique resource for ethical research into genetic and environmental factors that impact on human health and disease, to improve the health of future generations."[221] The bank is to be a resource of information for investigating the "causes, courses, and treatments of the common severe illnesses, and improving ways of dealing with them,"[222] and access to its collections will be granted to both research institutions and commercial companies in order to facilitate research and promote sharing of data and findings.[223]

Unlike the Icelandic Health Sector Database, the U.K. Biobank will operate on the basis of explicit consent,[224] and volunteers will be recruited on the basis of an opt-in regime.[225] However, conditional consent – consent that allows participants to choose which part of the data will be used, by whom, and for what purposes – will not be available because of the difficulty of implementing this framework in such a large scale database.[226] In the words of the Interim Advisory Group on Ethics and Governance that accompanies the project: "participation will have to be all or nothing

---

[219] *See id.*

[220] Interim Advisory Group on Ethics and Governance, *UK Biobank Ethics and Governance Framework, Background Document*, 3, 7 (October 10, 2003) available at http://www.ukbiobank.ac.uk/docs/egf-background.doc (last visited January 2006); J.V. McHale, *Regulating Genetic Databases: Some Legal and Ethical Issues*, 12 MEDICAL LAW REVIEW 70, 78 (Spring 2004).

[221] *See* The U.K. Biobank website at http://www.ukbiobank.ac.uk (last visited January 2006).

[222] The U.K. Biobank Ethics and Governance Framework, Setting Standards, 1 (September 24, 2003) available at http://www.ukbiobank.ac.uk/docs/egf-summary.doc (last visited January 2006).

[223] Interim Advisory Group on Ethics and Governance, *supra* note 220, at 12-13.

[224] *Id.*, at 6-7 stating: "The EGF [Ethics and Governance Framework] construes consent as 'consent to participate in UK Biobank'…For contemplated uses of data or samples, or kinds of data or sample collection, for which existing consent does not apply, new consent must be sought."

[225] Alan Doyle, Frances Rawle, & Peter Greenway, *The U.K Biobank* in SOCIETY AND GENETIC INFORMATION: CODES AND LAWS IN THE GENETIC ERA 247, 247 (Judit Sándor ed., 2003); McHale, *supra* note 220, at 73.

[226] Petersen, *supra* note 9, at 285.

– i.e., participants will have to be either *in* or *not in* U.K. Biobank" (emphasis in original).[227]

Notwithstanding this limitation, the participants in the project would have the right to withdraw from it at any time.[228] The U.K. Biobank Ethics and Governance Framework (EGF) recognized three possible degrees of withdrawal: complete withdrawal that includes a request to destroy samples already collected; discontinued participation, meaning that no further data will be collected but continuous use of existing data will be permitted; and lastly, a request that no further contact and communication will be made with the participant, although the data already collected remains in the database.[229] The EGF concludes that "the principle of voluntaries requires that participants be allowed to withdraw with little effort, at any time, and without having to give a reason."[230]

In contrast to the commercial approach taken in the Icelandic HSD Act, which grants a private company exclusive control over the Health Sector Database, the U.K. Biobank project is funded by: the Wellcome Trust, a medical research charity; two governmental institutions: the Medical Research Council (MRC), and the Department of Health; and the Scottish Executive, the devolved government of Scotland.[231] The U.K. Biobank is publicly owned and is monitored by an independent body, the Ethics and Governance Council.[232] This construction was designed to gain the public trust[233] and it strives to promote an ongoing engagement with the public.[234]

---

[227] Interim Advisory Group on Ethics and Governance, *supra* note 220, at 6-7.
[228] *Id.*, at 5; Doyle, Rawle, & Greenway, *supra* note 225, at 259-260.
[229] Interim Advisory Group on Ethics and Governance, *supra* note 220, at 10.
[230] *Id.*, at 10.
[231] *See* http://www.ukbiobank.ac.uk/ (last visited January 2006).
[232] For a chart of the UK Biobank organization, funding, and management structure *see* http://www.ukbiobank.ac.uk/about/management-structure_files/slide0004.htm (last visited January 2006).
[233] Doyle, Rawle, & Greenway, *supra* note 225, at 262-263.
[234] Interim Advisory Group on Ethics and Governance, *supra* note 220, at 9.

Another difference from the Icelandic model is that no party will be granted exclusive access to the U.K. database.[235] Academic as well as commercial institutions will have access to the database based on a case-by case evaluation of the research proposals and conditional upon adherence to the ethical framework of the project.[236]

The sample collection and the database will be legally owned by U.K. Biobank Limited. This means that participants in the project will not have property rights in the samples they provide and that U.K. Biobank retains the right to sell or destroy the samples and data.[237] Even though the EGF states that U.K. Biobank Ltd. does not intend to exercise these rights, such as the right to sell the samples and data, designating the U.K. Biobank to be a trustee of the samples and information collected, rather than the owner, would have been more appropriate. In addition, the definition of a trustee better fits with the stated intention to serve as a "steward of the resource, maintaining and building it for the public good" as emphasized in the Ethics and Governance Framework.[238]

One of the main questions that the U.K. Biobank still faces is who should be granted access to the information collected via this project. Commercial companies, employers, and the insurance industry are all examples of problematic recipients of the data. The U.K. Human Genetics Commission supports the view that employers and insurers should not have access to individual genetic information in order to prevent the misuse of the data collected and the privacy interests of the participants.[239] Similarly, the police or other law enforcement agencies will have access to the database only under a court order so as to not deter public participation.[240] However,

[235] Interim Advisory Group on Ethics and Governance*, id.*, at 12.
[236] *Id.,* at 12.
[237] The U.K. Biobank Ethics and Governance Framework, *supra* note 222, at 3.
[238] *Id.*, at 3.
[239] U.K. Human Genetics Commission, *supra* note 28.
[240] The U.K. Biobank Ethics and Governance Framework, *supra* note 222, at 3.

commercial companies could gain access to the data if the ethical framework set by the EGF is followed.

All identifying information, such as name and address, will be removed and kept separately from the information and samples, which will be coded.[241] Research users will only have access to anonymized data and samples and only a minimal number of people will have access to the key and will be able to re-identify the information.[242]

This model, which rejects the public-private, commercial collaboration seen in Iceland and promotes a public-charitable approach, bestows data-subjects greater control over their personal information and its uses. Moreover, while the Icelandic model followed a top-down approach in order to address public concerns, the United Kingdom has followed a "partnership approach" aiming to work with the public.[243]

Nevertheless, the U.K. model is not free of criticism.[244] Concerns include the potential ability to link the genetic and health information stored in the database with other data such as police or employment records; the possibility that the project would undermine the public trust in medical research; and the worry that the project is politically conceived, and hence has questionable scientific efficiency.[245] The project has also been criticized for permitting the disclosure of future medical records, which may be yet unknown to the research subject, under its informed consent policy.[246] Despite these concerns, this charitable model, compared to the Icelandic commercial model, seems to better protect the privacy and autonomy interests of the data subjects while nonetheless striving to enhance scientific knowledge.

---

[241] *Id*.,at 3.
[242] The U.K. Biobank Ethics and Governance Framework, *id*., at 3.
[243] *See* Beatrice Godard et al., *Strategies for Consulting with the Community: The Cases of Four Large-Scale Genetic Databases*, 10(3) SCIENCE AND ENGINEERING ETHICS, 1 (2004).
[244] *See* Petersen, *supra* note 9, at 278.
[245] *Id*.
[246] Rothstein, *supra* note 87, at 93‑94.

The U.K. model is preferable to the Icelandic one in several aspects. First, it rejected a market-type model. While the Icelandic database is ran by a private company that has exclusive control over it, the U.K. biobank is owned by U.K. Biobank Limited, a company established by governmental and charitable bodies for this purpose alone. This type of governance is better suited to the task, as it is less subject to conflicting forces and has the public's best interest at heart, rather than the promotion of shareholder profits. Second, the U.K. model better reflects the will and autonomy of the population as it chose an opt-in framework, rather than the opt-out model available under the Icelandic HSD Act. In addition, the U.K. model promises an explicit consent format, which better reflects the autonomy of the participants compared to the "blanket consent" granted to deCode in Iceland, although still raises concerns as to the ability to truly consent to the disclosure of unknown future medical conditions.

The fact that U.K. Biobank Limited retains ownership rights over the information and samples stored in the database, including the right to sell or destroy them, is also problematic. A preferable approach would be to treat U.K. Biobank Ltd. as a trustee of the information, rather than the owner, with clear limitations including restrictions on the right to sell, transfer, reveal, and destroy the information to third parties other than for the research purposes agreed to by the participants and authorized by an independent review board.[247] These limitations are essential if adequate degree of control and protection is to be given to genetic privacy and to the autonomy of the participants of the project.

[247] *See also supra* note 144 and the accompanying text.

D. Inductions for the U.S.

The Icelandic as well as the British experiences should serve as a compass for the United States in its future treatment of personal genetic information. The Icelandic model demonstrates some of the potential dangers and the privacy breaches resulting from granting private commercial companies extensive control over medical and genetic information, including information initially collected by public authorities before the creation of the database.[248] The British model, on the other hand, raises concerns as to the need to limit the power and control held by the government and public institutions that are collecting and handling medical and genetic information and material.[249] Absent formal limitations and constraints, these institutions are not restrained from destroying data collected or transferring their medical and genetic collections to third parties even without the consent of the individuals to whom the information pertains.[250] These concerns should be addressed in future treatment of genetic information and genetic privacy, particularly as science advances and more personal information could be gained from our genes.

At this point in time, it is unlikely that the private sector in the United States will cease to collect and store genetic information. For this reason, greater supervision of the conduct of the private sector must take place, limiting the control private companies have over personal genetic information and material and empowering the individuals to proactively control this information. Placing constraints on the private sector may be done in two different ways. The first is by introducing formal, top-down regulations enforced by the government. The second requires the industry to place limitations on itself in the form of specifically designed fair information

[248] *See* section III.A.
[249] *See* section III.C.
[250] *See supra* note 237 and the accompanying text.

practices that will deal with the various privacy and autonomy concerns that accompany genetic databases as raised throughout this article.

Self-regulation in the form of fair information practices has many advantages over government regulation, including speed and simplicity.[251] Moreover, a regime of fair information practices has in past experiences been successful in protecting information privacy.[252] Hence, at this point, fair information practices that encompass the uniqueness of genetic information and appropriately address issues of anonymity, usage, and security may be well suited to the task.[253] It is recommended that all institutions that collect, store, or manage genetic or medical information, either in the form of databases or biobanks, adopt the following principles as a basis for their privacy policies:

Opt-in Regime: The most basic way to insure that data subjects know and agree to be part of a genetic database or a biobank is to have them actively consent to it. This is especially important since genetic databases and biobanks may contain most private and sensitive information and it is necessary that each individual participating in such projects be aware of her participation and consent to it. The best way to achieve this is by adopting an opt-in framework, which requires active consent of individuals prior to adding them into the database/bank. In contrast, an opt-out regime does not insure these important goals, but rather perpetuates an existing situation.

Informed Consent: Data subjects should be asked to give explicit informed consent to the uses of the data collected. The British model and the Icelandic model, as previously explained, serve as prototypes for different degrees of informed consent.

---

[251] *See also* section II.C.

[252] *See* Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get)*, 2001 STANFORD TECHNOLOGY LAW REVIEW 1, 44-46 (2001). For a different view *see* Campbell, *supra* note 91, concluding that self-regulation did not live up to its expectations when applied to digital television public interest responsibilities and to privacy protection on the internet.

[253] *See also* Samuelson, *supra* note 117, at 1169.

Analysis of these two models favors the explicit informed consent framework adopted in the British model compared to the weaker alternative adopted by the HSD Act.

Withdrawal: Each participant in genetic databases or biobanks should be given the opportunity to withdraw its participation in the database at any given time. Withdrawal should be accompanied with the possibility to request the deletion or destruction of information and material already existing in the database/biobank. Once again, the British biobank, which better serves this goal compared to the Icelandic database, could serve as an appropriate model.

Security: Strict and coherent means of security should be implemented to safeguard the information collected, including its encryption. Only coded information should be transferred from public to private entities and the decoding key and identifiable information must remain with the original holder, unless the individual consented otherwise.

Confidentiality: Researchers should take strict measures to insure that the privacy and confidentiality of data subjects are kept. Identifiable information should be coded and kept separate from the samples collected. Only a limited number of people should have access to the identifiable information or to the decoding key. Privacy policies should be adopted and followed by each institution.

Ownership: Each privacy policy should be clear as to whether the holders of the information view themselves as owners, holding property rights over it, or simply as trustees of the information. The latter is viewed as more fit to this domain, and is hence preferable. If, however, a property rights regime is maintained, it is crucial to

place clear restrictions on the use of the data collected in addition to limiting transferability.[254]

Information Transfer: Each privacy policy should be explicit as to its stance towards information transfer to third parties. It is recommended that clear limitations be placed in this regard. Specific guidelines should be construed to provide answers to situations that include transfer of information outside the national borders and that level of privacy protection that must be maintained by the new holder. In any event, transfer of identifiable information should not take place absent the explicit consent of the data subjects.

Information Sharing: It is further advised that institutions that hold genetic information or material follow an explicit policy that refrains from transferring or revealing sensitive information to entities such as insurance companies or employers that may make use of such information for discrimination purposes. Similarly, it is recommended not to mix military or criminal databases with research ones absent the explicit consent of the research subjects so as to maintain the public trust.

Accountability: Lastly, it is crucial that institutions or personnel that breach these principles be held accountable for their actions. In order to ensure this it may be useful to have some type of government supervision on the conduct of entities holding such sensitive information in addition to industry compliance mechanisms.[255]

In addition to this set of principles and notwithstanding the importance of self-regulation, government involvement is not to be dismissed. The fact that several private companies chose to adhere with the HIPPA regulations even when claiming

[254] The latter is an application of the "Hybrid inalienability" model proposed by Paul Schwartz. *See* Schwartz, *supra* note 12, at 2090-2094.

[255] Schwartz identifies three purposes for which supervising institutions are needed: 1) to provide trading mechanisms; 2) to verify claims to propertized personal data; and 3) to police compliance with the agreed-upon terms. *See* Schwartz, *supra* note 12, at 2110.

they were not obliged to do so,[256] illustrates the power of government participation and its significance in the works of the private sector. The government can and should encourage the private sector to adopt these principles and practices by providing economic incentives to those who comply and by policing the conduct of the institutions.

One issue discussed above specifically calls for government regulation and should not be left to self-regulation alone. That is the mandate granted to the private sector over medical and genetic information and material and the freedom granted by it to transfer the information to third parties without any limitations. The private industry cannot be viewed as the owner of the medical and genetic information and material it collects for transferring purposes;[257] but rather, it should be legally defined as a trustee of the information and samples collected.[258] Under this mechanism, private companies as well as public institutions will not be banned from transferring their medical and genetic collections to a third party, but rather would be required to receive explicit consent from each individual whose information is included in the database prior to taking such meaningful steps. This will restore the control of the individuals over their personal genetic information and will ensure individual knowledge and agreement to the whereabouts of their personal genetic information and its uses.

[256] *See supra* note 133 and the accompanying text.
[257] The discussion above does not refer to the issue of ownership for intellectual property purposes. Ownership by physicians, researchers, and companies for intellectual property purposes over genetic discoveries derived from genetic material collected from volunteers, calls for a different analysis that is out of the scope of this article.
[258] *See also supra* note 144 and the accompanying text.

CONCLUSION

This article examines the emergence of public and private genetic databases and bio-repositories as well as the newly formed partnerships between the public and private sectors in the genetic realm. It calls for a prompt establishment of industry-wide fair information practices for assembly, storage, use, and safeguarding of genetic data, in order to adequately protect personal genetic privacy and autonomy.

Lack of adequate limitations enable the private sector to gain growing, almost unlimited, control over personal genetic information and material, while ignoring the privacy and autonomy rights and needs of data subjects. Taking privacy and autonomy of the research subjects seriously is not meant to undermine research but rather safeguard research subjects from possible misuses and establish public trust that is crucial for future scientific endeavors. The best and quickest way to insure the credibility of genetic databases and biobanks, and to protect the privacy and autonomy of data subjects, is by adopting and implementing fair information practices as suggested.