Immortal Invasive Initiatives? The Need for a Genetic "Right to Be Forgotten"

Thomas Hale-Kupiec
Note

Immortal Invasive Initiatives? The Need for a Genetic “Right to Be Forgotten”

Thomas Hale-Kupiec*

INTRODUCTION

In January 2015, President Barack Obama proposed spending $130 million to create a population-scale study at the National Institutes of Health (NIH). This study aims to create a database containing health information with genetic, environmental, lifestyle, medical, and microbial data from over two million participants. This note proposes that as a result of recent Supreme Court holdings eroding rights to personal privacy and gaps in federal privacy and information laws, the United States should consider adopting the European “Right to Be Forgotten” solely within the context of genetic information. The note begins by laying out the details of the President’s forthcoming Precision Medicine Initiative (PMI or the Initia-

© 2016 Thomas Hale-Kupiec
* J.D. Candidate, 2015, University of Minnesota Law School, M.P.H. Graduate, 2013, George Washington University. An extraordinary “thank you” must be given to Professor William McGeveran at the University of Minnesota for his advice and guidance on this note. Without him, this article could not have been completed in a timely fashion.


This note then reviews why this use of information is exceptional, relative to other forms of information, and explores the relationship that DNA information has had with human rights (from both a historical and a bioethical perspective).

Next, looking to civil and criminal case law, this note analyzes current issues associated with an existing, centralized DNA database. Finally, this note reviews the European “Right to Be Forgotten,” and analyzes how this right may be useful in the implementation of the new Precision Medicine Initiative. The note concludes with a discussion of public health and public policy arguments that would justify the “Right to Be Forgotten” for this limited context.

A. THE PRECISION MEDICINE INITIATIVE

In January 2015, President Barack Obama proposed spending $215 million on the Precision Medicine Initiative. The largest part of the money, $130 million, would go to the National Institutes of Health in order to create a population-scale study.

This study would create a database containing health information with genetic, environmental, lifestyle, medical, and microbial data from both healthy and sick volunteers with the aim that it will be used to accelerate medical research and to personalize treatments to patients. This database’s immediate purpose, as noted by the NIH, “will be to significantly expand efforts in cancer genomics to create prevention and

4. See Giusti, supra note 1.
5. See infra notes 23–108 and accompanying text.
6. See infra notes 113–143 and accompanying text.
7. See infra notes 144–170 and accompanying text.
8. Williams, supra note 3.
10. See Burton, Rockoff & Winslow, supra note 9; Regalado, supra note 9.
treatment successes for more cancers.”

More long-term goals include “researchers understand[ing] how genomic variations and other health factors affect the development of disease.” Some physicians believe these objectives could come to fruition, and subsequently, could offer more targeted, personalized patient care resulting in a healthier population, however other physicians are skeptical, considering the findings of previous government initiatives. Regardless of feasibility, though, the political and financial components of this project seem to have been established with little to no opposition.

So why is there any concern over this project, when three major patient protections in federal law—the Common Rule,

14. Fred N. Pelzman, Making Medicine More Personal, MEDPAGE TODAY (Feb. 12, 2015), http://www.medpagetoday.com/PatientCenteredMedicalHome/PatientCenteredMedicalHome/49997 (“We’ve all seen patients who live their entire lives with incredibly high blood pressures, who never have a stroke, heart failure, kidney failure, or a heart attack. Personalized medicine can potentially show us this: Which patient will develop high blood pressure. Which patients are salt responsive. Which patient will respond to which medicine. Which patients’ blood pressure, left uncontrolled, will lead to end-organ damage down the road . . . . No one is going to be better positioned to help administer this . . . than the primary care providers.”).
15. Michael J. Joyner, ‘Moonshot’ Medicine Will Let Us Down, N.Y. TIMES (Jan. 29, 2015), http://www.nytimes.com/2015/01/29/opinion/moonshot-medicine-will-let-us-down.html?ref=opinion&_r=2 (“But for most common diseases, hundreds of genetic risk variants with small effects have been identified, and it is hard to develop a clear picture of who is really at risk for what. This was actually one of the major and unexpected findings of the Human Genome Project. In the 1990s and early 2000s, it was thought that a few genetic variants would be found to account for a lot of disease risk. But for widespread diseases like diabetes, heart disease and most cancers, no clear genetic story has emerged for a vast majority of cases . . . . We would be better off directing more resources to understanding what it takes to solve messy problems about how humans behave as individuals and in groups. Ultimately, we almost certainly have more control over how much we exercise, eat, drink and smoke than we do over our genomes.”).
16. See Id.
the Health Insurance Portability Privacy Rule (HIPAA), and the Genetic Information Nondiscrimination Act (GINA)—are already in place? Aside from legal concerns, there are both historical and ethical concerns with collecting genetic information that are not addressed by existing laws.

---

18. The Privacy Rule, U.S. DEPT HEALTH & HUM. SERVS., http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/ (last visited Oct. 14, 2015) (“The HIPAA Privacy Rule establishes national standards to protect individuals’ medical records and other personal health information and applies to health plans, health care clearinghouses, and those health care providers that conduct certain health care transactions electronically. The Rule requires appropriate safeguards to protect the privacy of personal health information, and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patients rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections. The Privacy Rule is located at 45 CFR Part 160 and Subparts A and E of Part 164.”).

19. Genetic Information Discrimination, U.S. EQUAL EMP. OPPORTUNITY COMMISSION, http://www.eeoc.gov/laws/types/genetic.cfm (last visited Oct. 14, 2015) (“Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA) . . . took effect on November 21, 2009. Under Title II of GINA, it is illegal to discriminate against employees or applicants because of genetic information. Title II of GINA prohibits the use of genetic information in making employment decisions, restricts employers and other entities covered by Title II (employment agencies, labor organizations and joint labor-management training and apprenticeship programs - referred to as ‘covered entities’) from requesting, requiring or purchasing genetic information, and strictly limits the disclosure of genetic information. The EEOC enforces Title II of GINA . . . The Departments of Labor, Health and Human Services and the Treasury have responsibility for issuing regulations for Title I of GINA, which addresses the use of genetic information in health insurance.”).


21. See infra notes 23–80 and accompanying text.

22. See infra notes 81–109 and accompanying text.
B. HISTORICAL CONCERNS STEMMING FROM THE EUGENICS MOVEMENT

Current ethical, legal, and policy developments concerning human genetics cannot be understood without reference to the unique historical underpinnings stemming from the eugenics movement.23 Even still, some advocates analogize the “current revolution in molecular biology . . . to modify the pattern of human heredity for the better” to “[t]he eugenics movement of 1870-1950.”24 Regardless of historical uniqueness or continuity, there is growing popular interest in issues surrounding genetic privacy, as seen in the popularity of the recent book *The Immortal Life of Henrietta Lacks*,25 which was named a “Notable Book of the Year” by the *New York Times*.26 The book follows a tumor tissue sample taken from Ms. Lacks without her consent; her cells in this sample could divide indefinitely, ultimately leading to their use in hundreds of scientific experiments in the following decades.27 The book’s popularity highlights an ever-increasing public concern about the implications of immortality through the either consensual or nonconsensual dispersion of one’s genetic material, in spite of the benefits such dispersion can offer.

Though the origin of eugenics can find some foundation in Charles Darwin’s *The Origin of Species* (some authors would note that historical traces can be found as far back as the

27. SKLOOT, supra note 25, at 4 (“Scientists had been trying to keep human cells alive in culture for decades, but the all eventually died. Henrietta’s were different: they reproduced an entire generation every twenty-four hours, and they never stopped . . . . If we went to almost any cell culture lab in the world and opened its freezers . . . we’d probably find millions—if not billions—of Henrietta’s cells in small vials on ice. Her cells were part of research into the genes that cause cancer and those that suppress it; they helped develop drugs for treating herpes, leukemia, influenza, hemophilia, and Parkinson’s disease . . . . Their chromosomes and proteins have been studied with such detail and precision that scientists know their every quirk.”).
Greek city states\textsuperscript{28}, the true pioneer of modern eugenic theory was Francis Galton with his work in \textit{Inquiries into Human Faculty and its Development.}\textsuperscript{29} Galton's work influenced two Americans: Charles Davenport, a member of the National Academy of Sciences, and Harry Hamilton Laughlin, an activist who used the research of Davenport to strategize the American eugenics movement.\textsuperscript{30} Both men advocated for tying research on human genetics, specifically the newly rediscovered work of Gregory Mendel on genetic inheritance, to eugenics in order to provide the eugenics movement with the requisite scientific legitimacy necessary to promulgate scientific policy.\textsuperscript{31} As a result of their activism, “[l]ocal eugenics societies and groups sprang up around the United States after World War I, with names such as the Race Betterment Foundation.”\textsuperscript{32} “Not only did eugenicists promote better breeding, they wanted to prevent poor breeding or the risk of it. That meant keeping people with undesirable traits in their heritage (including alcoholism, pauperism, or epilepsy) separate from others or, where law allowed, preventing them from reproducing.”\textsuperscript{33} Laws mandating vasectomy were first advocated for,\textsuperscript{34} followed by laws mandating sterilization.\textsuperscript{35} After World War I, the movement began to flourish; by 1926, seventeen states had eugenic sterilization laws.\textsuperscript{36}

\textsuperscript{28} David J. Galton, \textit{Greek Theories on Eugenics}, 24 J. MED. ETHICS 263–67 (1998) (“Plato’s works do reveal a profound interest in eugenics as a means of supplying the city state with the finest possible progeny.”).

\textsuperscript{29} Philip R. Reilly, \textit{Eugenics, Ethics, Sterilization Laws}, in 1 ENCYCLOPEDIA OF ETHICAL, LEGAL, AND POLICY ISSUES IN BIOTECHNOLOGY 204, 205 (Thomas H. Murray & Maxwell J. Mehman eds., 2000) (“Galton . . . began investigating the inheritance of talent among eminent English families about 1864. He coined the term eugenics . . . in 1883 in \textit{Inquiries into Human Faculty and its Development}. Public interest in the notion that the success and failure in life might be closely tied to the germ plasm that one inherited grew rapidly . . . . In 1904 . . . Galton drafted an official definition of ‘natural eugenics’ as ‘the study of the agencies under social control that may improve or impair the racial qualities of future generations either physically or mentally.’” (citations omitted)).

\textsuperscript{30} \textit{Id.}

\textsuperscript{31} \textit{Id.}


\textsuperscript{33} \textit{Id.}

\textsuperscript{34} Reilly, supra note 29, at 206.

\textsuperscript{35} \textit{Id.} at 206–07.

\textsuperscript{36} \textit{Id.} at 207–08.
Buck v. Bell[^37] marked the major affirmation of these laws. A forced sterilization law in the State of Virginia provided that:

- the health of the patient and the welfare of society may be promoted in certain cases by the sterilization of mental defectives, under care-
  ful safeguard . . . who if now discharged would become a menace but
  if incapable of procreating might be discharged with safety and be-
  come self-supporting with benefit to themselves and to society.^[38]

Carrie Buck, the plaintiff, was found “feeble minded” by the State of Virginia by nature of her birth and based on an alleged “record during life of immorality, prostitution, and untruthful-

...ess; had never been self-sustaining; and has had one illegiti-

tate child . . . supposed to be mental defective.”[^39] The evidence at trial was based on findings that “[h]er mother, Emma Buck, ‘was maritally unworthy; having been divorced from her hus-

band on account of infidelity . . . and has had one illegitimate

cild and probably two others inclusive of Carrie Buck;”[^40] test-

imony of eight witnesses near the area surrounding Carrie

Buck’s home; and two Virginia physicians.^[41] The counsel for the superintendent of the state institution attempted through this mix of expert opinion and character evidence to show “social inadequacy” and subsequently uphold Buck’s forced steriliza-

tion under the Virginia sterilization law.^[42] The counsel for Car-

rie Buck—who was a former director of the state institution seeking sterilization—called no witnesses, and records not pre-

sented at trial showed that almost all of the allegations con-

cerning Carrie Buck’s character or morals were actually un-

true.^[43] Rather, she, like many unwed mothers of that time, was

institutionalized in the first place to prevent further shame to the family.^[44] The Supreme Court, however, came to the conclusion that “[t]hree generations of imbeciles are enough” and af-

[^38]: Id. at 205–06.
[^40]: Id. (quoting Albert Priddy from a deposition in the trial record available to the Supreme Court).
[^41]: Id. at 50.
[^42]: Id. at 50–53.
[^43]: Id. at 50–54.
[^44]: Id. at 54 (noting that Carrie Buck was originally committed because she became pregnant after her foster parent’s nephew had raped her); Paul Lombardo, Eugenic Sterilization Laws, COLD SPRING HARBOR LABORATORY, http://www.eugenicsarchive.org/html/eugenics/essay8text.html (last visited Oct. 14, 2015).
firmed the mandatory sterilization of Carrie Buck on the grounds of public good. The legality of these laws resulted in widespread public comfort regarding morally ambiguous laws. Legality of the statutes concerning eugenics failed to change until nearly fifteen years later with Skinner v. Oklahoma. In Skinner, the Supreme Court finally overruled an Oklahoma statute allowing for “habitual criminals” to be “rendered sexually sterile” if done “without detriment to his or her general health.” The Court, pursuant to public policy, found that “[m]arriage and procreation are fundamental to the very existence and survival of the race” and stated that procreation “involves one of the basic civil rights of man.” As a result, the Supreme Court held that the “depriv[ation] of a basic liberty” cannot be justified, and subsequently had to strike down the state law on Fourteenth Amendment grounds.

1. Racial and Prejudicial Exploitation

Though the Personalized Medicine Initiative is not seeking to directly control populations like the eugenics movement, the historical underpinnings inherent in population-based research are important for a variety of reasons. First, when discussing the government policies concerned with genetics and health, the historical context of exploitation of one population at the whim of another is important. Historical recognition that

46. See ANDREWS, MEHLMAN & ROTHSTEIN, supra note 23, at 64 (discussing, for example, how from 1917 to 1983, the state of Oregon forced more than 2,500 Oregonians to be sterilized).
48. Id. at 537.
49. Id. at 541.
50. Id.
51. Id. (“When the law lays an unequal hand on those who have committed intrinsically the same quality of offense and sterilizes one and not the other, it has made as invidious a discrimination as if it had selected a particular race or nationality for oppressive treatment.”).
52. See generally Michael Yudell, A Short History of the Race Concept, in RACE AND THE GENETIC REVOLUTION: SCIENCE, MYTH, AND CULTURE 13, 21 (Sheldon Krimsy & Kathleen Sloan eds., 2011) (“Yet, despite the best intentions by scientists . . . to reconceptualize the concept of race for modern biology, evidence suggests that these geneticists and their scientific allies ultimately helped to preserve the concept of race in science, and hence for use by both scientific and nonscientific racists—its methodological utility to evolutionary
some subpopulations have been forced to comply with statutes that may be buttressed with weak “scientific” correlations is essential to understand the privacy considerations central in modern scientific policy.\textsuperscript{53} The Initiative, as such, should continue its current regimen of substantial disclosure concerning the justifying science before moving to drastic goals or polices.\textsuperscript{54}

In conjunction, legally tolerated selective breeding resulting from private (rather than public) decision-making continues to flourish in the United States.\textsuperscript{55} Currently, the only federal law concerning in vitro fertilization (IVF) services is the Fertility Clinic Success Rate and Certification Act of 1992,\textsuperscript{56} which merely requires infertility clinics to report success rates in a standardized fashion; further, state regulations of these clinics are minimal.\textsuperscript{57} The rise of correlations stemming from these data on health populations from the Personalized Medicine Initiative could further advance the aforementioned stigmas and, in particular, drive racial bias.\textsuperscript{58} In conjunction, private family planning initiatives,\textsuperscript{59} reversible contraceptive services and

biologists and population geneticists would quickly be exploited and manipulated by these racists.

\textsuperscript{53} See generally id.

\textsuperscript{54} DIXIE BAKER ET AL., NAT’L INST. HEALTH, PARTICIPANT ENGAGEMENT, DATA PRIVACY, AND NOVEL WAYS OF RETURNING INFORMATION TO PARTICIPANTS 5 (2015), [https://web.archive.org/web/20151005053135/http://www.nih.gov/precisionmedicine/whitepapers/Participant-Engagement-Data-Privacy-Returning-Information.pdf] (stating that a goal of the Initiative is to “Develop novel ways to communicate, inform, and educate the public about research and health issues broadly, which will build capacity for an engaged and informed public. Increased public comfort with the science underlying precision medicine will be important to prepare individuals to be partners in health care decisions down the road.”).

\textsuperscript{55} Maxwell J. Mehlman, Modern Eugenics and the Law, in A CENTURY OF EUGENICS IN AMERICA: FROM THE INDIANA EXPERIMENT TO THE HUMAN GENOME ERA 219, 222–23 (Paul A. Lombardo ed., 2011) (“Some of the most glaring selective breeding practices are associated with gamete donation . . . . A company called Fertility Alternatives pays a premium to ‘exceptional’ egg donors. To qualify, the donor must have graduated from a major university, or be currently attending one, preferably Ivy League; have a GPA of 3.0+; SAT scores of 1350+ or ACT scores of 30+; and have a documented high IQ.”).


\textsuperscript{58} See generally Yudell, supra note 52.

\textsuperscript{59} Mehlman, supra note 55, at 224 (describing one private family planning initiative in California called “Project Prevention (formerly CRACK)”
sterilization services aimed at the poor, could all be termed “neo-eugenic” practices. Thus, the government needs to ensure that information disclosures stemming from this Initiative control for racial or other prejudicial biases and narrowly tailor their outcomes to avoid inequitable treatment, noting that modern big data considerations and computer-generated algorithms “can mask prejudices while maintaining a patina of scientific objectivity.” Currently, the methods of the Initiative, at least those to identify and recruit cohorts, only list this concern, while failing to list a recommendation on how to reconcile it.

2. The Volume, Variety, and Velocity of Data Being Uploaded

The second major consideration necessary to incorporate relative to the eugenics movement is the government’s embrace of collecting large amounts of data on a population and then linking and aggregating other information sources to generate complex dossiers on individuals. Professor Gostin from Georgetown University Law Center conceptualizes the problem as follows:

that was started in 1997 and gave “drug addicts $200 if they undergo sterilization or use long-term birth control;” in 2003, the organization claimed “23 chapters nationwide and had paid 907 women,” of which “African Americans and Hispanics accounted for 401 of the participants”).

60. Id. at 227 (“[T]he government in 2001 spent $1.26 billion on reversible contraceptive services and $95 million on sterilization services. These funds are distributed through several programs . . . . [V]irtually all of these funds are earmarked for the poor.” (footnote omitted)).

61. Id. at 228–29 (“[T]he more children the taxing family has, the larger the number of credits that it can claim. The policy might be regarded as eugenic in that, since only families with enough income to pay taxes benefit from the credit, the policy creates an incentive for better-off families to have more children.”).

62. See id. at 224–33 (labeling as neo-eugenic a number of public and private efforts to encourage or discourage procreation among targeted groups based on perceived benefits to society).


65. See, e.g., BIG DATA, supra note 63.
The combination of emerging computer and genetic technologies poses particularly compelling privacy concerns. While this technology can markedly facilitate research, screening, and treatment of genetic conditions, it may also permit a significant reduction in privacy through its capacity to store and decipher unimaginable quantities of highly sensitive data. A variety of underlying harms to patients may result from unwanted disclosures of these sensitive genomic data.66

Linking various forms of data with an array of factors (including genetics) may present false correlations and may result in an increase in researchers asserting mistaken outcomes, arbitrary choices, or underestimate the high degree of uncertainty in the judgment it produces.67 Because it is the government that collects this personal information about an individual, these data are subject to a variety of regulations68 and constitutional protections. Yet, these once strong regulations have been eroded through recent Supreme Court cases regarding DNA repositories.69

Specifically, the magnitude of data being produced and collected is resulting in the initially-made protections being bypassed; in 2013, the world had surpassed an estimated four zettabytes of total stored data, while the one zettabyte marker had only been passed in 2010.70 The benefits of collecting mass amounts of data may be a good thing, but will depend on how data are interpreted and used.71 This said, with increasing vol-

67. BIG DATA, supra note 63, at 45–47.
68. See supra notes 17–19 and accompanying text.
69. See infra notes 113–170 and accompanying text.
70. John Gantz & David Reinsel, Extracting Value from Chaos, IDC (June 2011), http://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf; BIG DATA, supra note 63, at 2 (“A zettabyte is 1,000,000,000,000,000,000,000 bytes, or units of information. Consider that a single byte equals one character of text . . . . [I]magine that every person in the United States took a digital photo every second of every day for over a month. All of those photos put together would equal about one zettabyte. More than 500 million photos are uploaded and shared every day . . . 200 hours of video are uploaded every minute.”).
71. BIG DATA, supra note 63, at 7 (“For example, a genetic researcher at the Broad Institute found that having a large number of genetic datasets makes the critical difference in identifying the meaningful genetic variant for a disease. In this research, a genetic variant related to schizophrenia was not detectable when analyzed in 3,500 cases, and was only weakly identifiable using 10,000 cases, but was suddenly statistically significant with 35,000 cases. As the researcher observed, ‘There is an inflection point at which everything changes.’ The need for vast quantities of data—particularly personally sensitive data like genetic data—is a significant challenge for researchers for a
ume, variety, and velocity of data collected by the government about individual subjects, the opportunity and possibilities of correlation to certain prejudices or traits increasingly become a reality.72

That genetic information would be used to discriminate or oppress is not just a hypothetical issue. In response to increased concerns over genetic discrimination, Congress passed the Genetic Information Nondiscrimination Act (GINA), which protects against genetic information being used for any aspect of an employment decision,73 in prohibiting health insurance coverage in the individual market, or to establish rules for the eligibility (including continued eligibility) for any individual enrolling in an individual health insurance plan.74 However, GINA does not regulate other forms of insurance and does not protect a party after they develop a condition (sometimes termed “phenotypic penetration”) in either the health insurance or employment discrimination context.75 Further, with big

variety of reasons, but notably because of privacy laws that limit access to data. The data clusters and relationships revealed in large data sets can be unexpected but deliver incisive results. On the other hand, even with lots of data, the information revealed by big data analysis isn’t necessarily perfect. Identifying a pattern doesn’t establish whether that pattern is significant. Correlation still doesn’t equal causation. Finding a correlation with big data techniques may not be an appropriate basis for predicting outcomes or behavior, or rendering judgments on individuals. In big data, as with all data, interpretation is always important.”).

72. Cf. id.

73. Genetic Information Discrimination, supra note 19 (“The law forbids discrimination on the basis of genetic information when it comes to any aspect of employment, including hiring, firing, pay, job assignments, promotions, layoffs, training, fringe benefits, or any other term or condition of employment. An employer may never use genetic information to make an employment decision because genetic information is not relevant to an individual's current ability to work.”).


75. Russell Korobkin & Rahul Rajkumar, The Genetic Information Nondiscrimination Act — A Half-Step Toward Risk Sharing, 359 NEW ENG. J. MED. 335, 336 (2008) (“First, GINA not only fails to protect the person with colonic polyps; it actually leaves him worse off. . . . Because insurance companies may no longer make use of clearly relevant information such as family history in their risk assessment, they will rely even more heavily on current health status when setting rates, even when it has only slight value in predicting future illness. . . . Second, . . . those whose genes put them at lower risk can opt out entirely or, more likely, purchase insurance with higher deductibles, greater cost sharing, and more exclusions.”); Mark A. Rothstein, GINA's Beauty Is Only Skin Deep, GENEWATCH, Apr.–May 2009, at 9, 9–10, http://www.councilforresponsiblegenetics.org
data transmitting increasing amounts of personal information, it is increasingly possible that this genetic information could be somehow disclosed and, as a result, employers that have obtained genetic information could search for other justifiable factors to use to justify an adverse action. Further, from a public health perspective, disclosure of any sensitive health information may result in the inability to obtain insurance or employment which subsequently may raise an individual’s medical debt (leading to further public health issues) or keep regional unemployment rates high. Privacy concerns regarding DNA information have been increasing in recent [source](http://genewatch/GeneWatchPage.aspx?pageId=184) (“There are three major flaws with GINA. First, it applies only to two aspects of the problem, discrimination in health insurance and employment. GINA does nothing to prohibit discrimination in life insurance, disability insurance, long-term care insurance, mortgages, commercial transactions, or any of the other possible uses of genetic information. Second, GINA’s prohibition on genetic discrimination in health insurance is largely a mirage. HIPAA prohibits discrimination by group health plans on the basis of any health information. Third, the employment provisions of GINA are ineffective, but for different reasons. As with health insurance, the employment provisions only apply to individuals who are asymptomatic. GINA qualifies this by saying that employers can require the release of all medical information except genetic information. Because this information is commonly interspersed in medical records there is no practical way for the custodians of the health records (e.g., physicians, hospitals) to send only non-genetic information.”).

76. See [BIG DATA, supra note 63, at 2.](http://example.com)

77. The combination of big data and leaked genetic information could allow for genetic discrimination to occur, as it did in pre-GINA case where the court granted no relief to a plaintiff who alleged she was pushed into less desirable, lower-pay position after her employer learned of a genetic disorder. [Laws v. Pact, Inc., No. 98C8107, 2000 WL 777926, at *3–4 (N.D. Ill. Apr. 19, 2000)](http://example.com) (holding that a plaintiff “must establish that her disability impacted on the defendant’s decisions” after a plaintiff provided evidence that the “defendant began to scheme to terminate her” after finding out she had a high genetic predisposition for Huntington’s Disease; the employer, via spontaneously offering her a similar position instead, was, in the court’s words offering a “reasonable accommodation”).


times with the exploitation of gaps in these laws becoming more apparent.\textsuperscript{80}

C. MODERN BIOETHICAL CONCERNS

The Initiative seeks to combine data from “more than 200 large American health studies that are ongoing and together involve at least two million people.”\textsuperscript{81} Three major bioethical issues are implicated by this proposed database study: maintaining meaningful contact with participants to allow withdrawal of consent and report incidental findings; storing samples and data with adequate informed consent for later uses; and ensuring data remains secure.\textsuperscript{82}

First, maintaining contact with participants as to allow an ease of consent withdrawal may somewhat resolve problems of incidental findings in this Initiative. If the government conglomerates information from multiple studies or utilizes information beyond the scope of the original studies, the government may be bypassing what was initially consented to when participants agreed to enroll in the original study.\textsuperscript{83} In the context of the Precision Medicine Initiative, how the government presents consent issues to participants and asks for consent—given the number of potential uses and potential users of the database—is the main first issue. The government attempted to alleviate consent concerns through the “Common Rule.”\textsuperscript{84} Under the standards and norms of the Common Rule, “research subjects must be allowed to discontinue their participation at any time without penalty or loss of benefits to which they

\textsuperscript{80} See generally SHAH, supra note 20.
\textsuperscript{81} Regalado, supra note 9.
\textsuperscript{82} For a general critical discussion of sample biobanks in Canada, and Europe that obtain broad consent from participants to cover unforeseen future uses of data rather than dynamic consent, which involves iterative follow-up when later uses become known, see generally Kristin Solum Steinsbekk, Bjørn Kåre Myskja & Berge Solberg, Broad Consent Versus Dynamic Consent in Biobank Research: Is Passive Participation an Ethical Problem?, 21 EUR. J. HUMAN GENETICS 897 (2013).
\textsuperscript{83} For a general discussion of how informed consent rules and norms are derived from a different type of research than is relevant for biobanks, and how there is a need for different rules to address different bioethical issues, see generally Mark A. Rothstein, Expanding the Ethical Analysis of Biobanks, 33 J.L. MED. & ETHICS 89 (2005).
\textsuperscript{84} See generally supra note 17 for background on the Common Rule.
would otherwise be entitled.”85 However, in the context of a genetic database, applying the Common Rule is complicated by the fact that samples and data from a participant may already be distributed to secondary research users who did not collect the specimen from the participant.86 This concern is not just limited to uses by additional government researchers, private entities (or those entities exempt from these Federal regulations) may end up using the database or derivative research products, and these entities do not need to necessarily comply with the “Common Rule.”87 As a result, any future disclosures of the Initiative’s datasets to the public or to private, third party researchers not bound by the Common Rule could result in publically-disclosed personal information that is not available for this opting out. Similarly, deletion or removal of this information may be an issue if the program ever becomes discontinued, or if users opt-out—presuming they are even allowed to in the first place. “Options after closure include destroying the specimens, transferring them to another facility, or letting them sit unused in freezers.”88 These raise a multitude of questions about what to do with specimens and when level of consent should be implicated.89

86. See id.
87. See Erin Williams, Cong. Research Serv., RL31340, Federal Protection for Human Research Subjects: An Analysis of the Common Rule and Its Interactions with FDA Regulations and the HIPAA Privacy Rule 6, 10–11, 18–19 (2005), http://fas.org/sgp/crs/misc/RL32909.pdf (noting the Common Rule applies to the eighteen departments and agencies doing and funding research, but “has not been adopted by all agencies that fund research” and would not necessarily apply to “research conducted without federal money” or “private companies”).
88. See R. Jean Cadigan et al., Neglected Ethical Issues in Biobank Management: Results from a U.S. Study, LIFE SCI. SOC’Y & POL’Y, Mar. 2013, at 1, 5–8 (reporting from a study of 456 U.S. biobanks that many often lack adequate planning for closure, and many samples are retained with hypothetical uses never becoming relevant).
89. See, e.g., id. at 9 (“[H]eighened expectations surrounding biobanks and other biotechnologies may cause people to set their hopes too high, while ignoring significant barriers, for what these technologies can offer future research . . . . [T]he discrepancy between biobankers’ optimism for results and . . . planning for termination, and specimen utilization, may inadvertently undermine transparency, informed consent, and ultimately, public trust.” (citations omitted)).
In line with bioethical issues around withdrawal of consent and termination of sample storage, major concerns exist for reporting incidental findings and individual research results that have potential health, reproductive, or personal importance to participants.\textsuperscript{90} No consensus yet exists on how to handle incidental findings in human subjects research,\textsuperscript{91} though some researchers have concluded that “researchers have an [ethical] obligation to address the possibility of discovering IFs [incidental findings] not only in their protocol and communications with the IRB [Institutional Review Board], but also in their consent forms and communications with . . . research participants.”\textsuperscript{92} These research efforts have yet to translate into explicitly stated legal duties.\textsuperscript{93}

Second, storing samples and data with adequate informed consent for later uses is an issue. Both collection and retention of this data is problematic; with this proposed Initiative, how the government ensures data collected remains secure both when in the hands of the government and researchers remains a serious issue. Questions on when, where, and how long this information is being held creates a vast array of bioethical and privacy concerns.\textsuperscript{94} Research on samples of human biological

\textsuperscript{90} See Susan M. Wolf et al., Managing Incidental Findings and Research Results in Genomic Research Involving Biobanks and Archived Data Sets, 14 GENETICS MED. 361, 365–70 (2012) (discussing unresolved issues and core bioethical questions for biobanks dealing with individual research results from research studies and incidental findings indicated or implied from research).


\textsuperscript{92} Susan M. Wolf et al., Managing Incidental Findings in Human Subjects Research, 36 J.L. MED. ETHICS 219, 227 (2008); see PRESIDENTIAL COMMISSION, supra note 91; Ofri, supra note 91.

\textsuperscript{93} See Tilson v. Ariz. State Univ. Bd. of Regents, No. 04-CV-1290, 2005 WL 6199562, at *2–6 (D. Ariz. Mar. 3, 2005) (dismissing claims for various tort damages by members of the Havasupai Indian Tribe whose blood samples had been provided to study diabetes rates, but were collected and stored under broad consent waivers and used for a variety of non-diabetes genetic research studies at Arizona State University).

\textsuperscript{94} See generally R. Jean Cadigan et al., “That’s a Good Question”: University Researchers’ Views on Ownership and Retention of Human Genetic
materials often occurs in two stages: initial collection and storage of samples and later research use and analysis of those samples. This gap between collection and analysis can pose a problem for informed consent as research needs and hypotheses evolve over time and may diverge from uses known and consented to at collection—this issue is especially pronounced for biobanks where longer storage periods are often involved. It has been suggested that to meet the ethical norms of informed consent when creating a biobank, participants should “be given comprehensive information about the repository (i.e., the collection of stored materials) itself, including details concerning its purpose, procedures, confidentiality protections, risks, and benefits.” Even when providing detailed information on anticipated research uses, biobanks often present a more complex issue, as future research or research proposals may not be available at the time of initial participant consent. To fully meet ethical norms, it has been proposed that “researchers should re-contact participants to obtain specific consent for each additional use,” but these follow-up consent contacts yield their own bioethical considerations, as participants may find “repeated contact to obtain consent for each study using their specimen may be seen as an unwelcome intrusion and a disincentive to participation.” A derivative concern when conducting repeated consent contacts may occur as participants may make assumptions about why they were included in a secondary study, and “may come to erroneous conclusions about why their specimens have been selected for the study of a particular gene or condition.” Any regime requiring re-contact and ex-

Specimens, 13 GENETICS MED. 569 (2011) (indicating that researchers often have misperceptions over who owns stored research samples and how ownership affects any associated stewardship obligations).

95. See McGuire & Beskow, supra note 85, at 362 (identifying the typical two stage research process as an opportunity for bioethical issues).

96. See, e.g., Steinsbekk, Myskja & Solberg, supra note 82.

97. McGuire & Beskow, supra note 85, at 363.

98. See id.

99. Id.; accord Rothstein, supra note 83, at 93 (”[T]he repeated recontacting of individual sample donors to solicit additional authorizations is likely to represent a greater intrusion on their privacy.”).

100. McGuire & Beskow, supra note 85, at 363 (citing Laura M. Beskow & Elizabeth Dean, Informed Consent for Biorepositories: Assessing Prospective Participants’ Understanding and Opinions, 17 CANCER EPIDEMIOLOGY BIOMARKERS PREVENTION 1440 (2008); Susanne B. Haga & Laura M. Beskow, Ethical, Legal, and Social Implications of Biobanks for Genetics Research, 60 ADVANCES GENETICS 505 (2008)).
plicit consent for each additional research use may result in increased costs, administrative burdens, and delays, and would likely diminish the value of the database and cause participants to drop-out which would have an “adverse effect on validity due to non-response and loss to follow-up.” 101 Again, how to deal with these concerns is hotly debated. 102

Finally, ensuring the security of this information is important as data breaches would violate participant consent and would lead to significant privacy and even personal ramifications. HIPAA should require protection of personally identifiable health information from a biobank, such that additional authorizations are required for later use or disclosure. 103 However, it is unclear when and how some of these established regulations are triggered in the case where information is thought to be disconnected or not individually identifiable, but is later found to be identifiable because information allowing re-connection of data has been incidentally released, or made available through an illegal data breach. 104 Some authors argue that genetic data cannot really be de-identified, and information stolen in a data breach could likely be re-identified using even basic metadata information and identity tracing techniques. 105 Although causes of action have developed in tort to allow protection of privacy, 106 and federal administrative a-

101. Id.

102. See, e.g., Mats G. Hansson et al., Should Donors Be Allowed to Give Broad Consent to Future Biobank Research?, 7 LANCET ONCOLOGY 266 (2006); Darren Shickle, The Consent Problem Within DNA Biobanks, 37 STUD. HIST. PHIL. BIOLOGICAL & BIOMEDICAL SCI. 503 (2006); Steinsbekk, Myskja & Solberg, supra note 82.

103. See Rothstein, supra note 83, at 93–94 (discussing the more strict requirements of HIPPA on biobanks than the requirements of the Common Rule).

104. See Rothstein, supra note 83, at 98 (noting that even a HIPAA non-covered entity, like a private sector biobank, “must comply with the requirements of HIPAA” because its data or specimens may have come “from a covered entity”).

105. Yaniv Erlich & Arvind Narayanan, Routes for Breaching and Protecting Genetic Privacy, 15 NATURE REV. GENETICS 409 (2014) (outlining a number of data breaching and data mining techniques that are used to conduct identity tracing attacks with basic demographic information and genetic information).

cies enforce statutes that attempt to ensure privacy and security of personal information.\textsuperscript{107} The rapid expansion of "big data"\textsuperscript{108} directly correlates to an increase in the potential for data breaches.\textsuperscript{109} While de-identifying data to remove potential bias by researchers is feasible, the ability of even the federal government to keep de-identified information from being re-connected to individuals is questionable in light of high profile data breaches—like the breach reported in 2015 of the Office of Personal Management’s databases of personnel and background check information on federal government employees, contractors, and other parties.\textsuperscript{110}

on behalf of members of the Havasupai Indian Tribe whose blood samples had been provided to researchers at Arizona State University to study diabetes rates, but were collected and stored under broad consent waivers and used for a variety of non-diabetes genetic research studies; see William L. Prosser, Privacy, 48 CALIF. L. REV. 383, 386–89 (1960) (noting the progression of state courts' recognizing a right to privacy and a claim for damages from invasion of privacy).

\textsuperscript{107} See, e.g., Dave & Buster’s Inc., 149 F.T.C. 1449, 2010 WL 9434816, at *1 (2010) (issuing an order under the Federal Trade Commission Act to force a restaurant chain to develop a network security system capable of preventing third party data breaches of credit card information); see also Data Security, FED. TRADE COMM’N, https://www.ftc.gov/tips-advice/business-center/privacy-and-security/data-security (last visited Oct. 15, 2015) (providing resources to businesses on their legal obligation to keep customer and employee personal information safe from data breaches). \textit{But see In re IPhone Application Litig.}, 844 F. Supp. 2d 1040 (N.D. Cal. 2013) (holding that mobile devices did not constitute facilities through which electronic communication service was provided under the Stored Communications Act (SCA), location data was not in “electronic storage” for purposes of the SCA, users’ geolocation data did not constitute “content” susceptible to interception under the Wiretap Act, and alleged disclosure of users’ unique device identifier number, personal data, and geolocation information did not violate users’ right to privacy); \textit{In re Jetblue Airways Corp. Privacy Litig.}, 379 F. Supp. 2d 299, 315 (E.D.N.Y. 2005) (holding that airline’s transfer of personal information of its passengers to the federal government following Sept. 11, 2001 was not a violation of the Electronic Communications Privacy Act (ECPA)).

\textsuperscript{108} See \textit{supra} notes 65–69 and accompanying text.


\textsuperscript{110} U.S. OFFICE PERS. MGMT., CYBERSECURITY RESOURCE CENTER: CYBERSECURITY INCIDENTS, https://www.opm.gov/cybersecurity/cybersecurity-incidents/ (last visited Dec. 7, 2015) (“In June 2015, OPM discovered that the background investigation records of current, former, and prospective Federal employees and contractors had been stolen. OPM . . . [has] concluded with high confidence that sensitive information . . . of 21.5 million individuals, was sto-
II. LEGAL ANALYSIS

The transition to a world of Big Data is forcing our conceptions of privacy to evolve, but there is still significant room to respect individual expectations of privacy, and there is no reason to believe that individuals will accept invasions to privacy just because “the novel methods of using data inherent in a computerized information system” (like the Initiative) “also allow novel methods of invading privacy.”

A. REPORTING SYSTEMS IN DNA RESEARCH (CIVIL CONCERNS)

In Whalen v. Roe, a New York law created a database of individuals receiving prescriptions for Schedule II drugs, including the names of the prescribing physicians. The law operated by requiring physicians to report the name of the “prescribing physician; the dispensing pharmacy; the drug and dosage; and the name, address, and age of the patient.” This information was then stored by the New York Department of Health in a heavily guarded location, and was retained for a period of five years. Public disclosure of the information was strictly prohibited and to prevent any disclosure, the state installed several safeguards to secure the data. At the district court level, the statutes were found to be an unconstitutional interference with a right to privacy under the fourteenth and

---

111. See generally BIG DATA, supra note 63.
113. Whalen v. Roe, 429 U.S. 589, 593 n.8 (1977) (“[Schedule II drugs] include opium and opium derivatives, cocaine, methadone, amphetamines, and methaqualone. These drugs have accepted uses in the amelioration of pain and in the treatment of epilepsy, narcolepsy, hyperkinesia, schizo-affective disorders, and migraine headaches.”).
114. Id. at 593.
115. Id. at 593–94.
116. Id. at 607 (Brennan, J., concurring) (“In this case, as the Court’s opinion makes clear, the State’s carefully designed program includes numerous safeguards intended to forestall the danger of indiscriminate disclosure. Given this serious and, so far as the record shows, successful effort to prevent abuse and limit access to the personal information at issue, I cannot say that the statute’s provisions for computer storage, on their face, amount to a deprivation of constitutionally protected privacy interests, any more than the more traditional reporting provisions.”).
enforcement of the law was enjoined.\textsuperscript{117} The Supreme Court reversed, holding that the statutes were within the state’s police power.\textsuperscript{118}

Justice Stevens, writing for the majority, held that enacting legislation attempting to mitigate crime, such as attempting to impact drug distribution, was within the state’s police power.\textsuperscript{119} When doing so, Justice Stevens noted two different privacy interests: “the individual interest in avoiding disclosure of personal matters,” and the ability to have “independence in making certain kinds of important decisions” free from government influence.\textsuperscript{120} Though he agreed these privacy interests may be affected by the New York statutes, Justice Stevens held that neither interest would be significantly impaired based on the high security installed by the New York Department of Health; because the increased risk of public disclosure was minimal compared to existing law; and because patients’ decisions to receive these drugs would be largely unaffected by having to provide identifying information.\textsuperscript{121} Justice Stevens went on to dismiss both the doctors’ and patients’ concerns as a result of the security protocol.\textsuperscript{122} Though he acknowledged the legitimate privacy concerns the plaintiffs had in the government database of personal information,\textsuperscript{123} Justice Stevens ended his opinion by limiting the holding to the specific facts in this case, that indicated New York’s program as a whole showed “a proper concern with, and protection of, the individual’s interest in privacy;” while the Justice noted that some other set of facts where the court did find “unwarranted disclosure of accumulated private data whether intentional or unintentional” could require a different analysis.\textsuperscript{124}

Justice Brennan wrote a concurring opinion, where he agreed that the required disclosure of patient information to select public health officials is a common and normal practice in healthcare that is historically prevalent and has not been

\textsuperscript{118} Whalen, 429 U.S. at 598.
\textsuperscript{119} Id. at 603–04.
\textsuperscript{120} Id. at 598–600.
\textsuperscript{121} Id. at 599–604.
\textsuperscript{122} Id. at 604.
\textsuperscript{123} Id. at 605 (“We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files.”).
\textsuperscript{124} Id. at 605–06.
traditionally considered an invasion of privacy.\textsuperscript{125} However, the “vast potential” of this information, he found troubling:

What is more troubling about this scheme, however, is the central computer storage of the data thus collected . . . . the Constitution puts limits not only on the type of information the State may gather, but also on the means it may use to gather it. The central storage and easy accessibility of computerized data vastly increase the potential for abuse of that information, and I am not prepared to say that future developments will not demonstrate the necessity of some curb on such technology.\textsuperscript{126}

\textit{Whalen v. Roe} involved a database of patients and information about their lawful use of prescription drugs that police wanted to monitor due to potential for unlawful uses.\textsuperscript{127} Diagnosis and disease data is often more sensitive than information about the lawful use of a prescription drug.\textsuperscript{128} The assembly of computerized database “systems increases both the number of users and the number of patient records.”\textsuperscript{129} The risk of invasion of privacy exponentially increases as the number of participants increase.\textsuperscript{130} “Most existing clinical information systems were designed and implemented without any significant analysis of protection of patient privacy;” when these systems were implemented, patient privacy was simply one of many factors to be balanced in implementing an efficient system design.\textsuperscript{131}

Bioethical considerations about appropriate uses of personal medical records also present legal hurdles. Informed consent may be an issue in this Initiative, considering that once samples are taken from unknowing patients\textsuperscript{132} or samples are

\begin{itemize}
  \item \textsuperscript{125} \textit{Id.} at 606 (Brennan, J., concurring).
  \item \textsuperscript{126} \textit{Id.} at 606–07.
  \item \textsuperscript{127} \textit{Id.} at 591 (majority opinion).
  \item \textsuperscript{128} Brannigan, \textit{supra} note 112, at 191–92 (“In many cases the problem is worse with clinical and research information systems”).
  \item \textsuperscript{129} \textit{Id.}
  \item \textsuperscript{130} \textit{See id. See generally Big Data, supra note 63.}
  \item \textsuperscript{131} Brannigan, \textit{supra} note 112, at 191–92 (describing hospital medical records systems before HIPAA); \textit{cf.} Sue Bowman, \textit{Impact of Electronic Health Record Systems on Information Integrity: Quality and Safety Implications, Persp. Health Info. Mgmt.}, Fall 2013 (noting a number of security and functionality issues with electronic health care records systems both in the design level, implementation level, and through widespread user errors).
  \item \textsuperscript{132} \textit{See, e.g., Moore v. Regents of the Univ. of Cal., 793 P.2d 479, 487 (Cal. 1990) (holding, on public policy grounds, that permitting a conversion law to encompass organs would hinder medical research, and noting that a patient can make an informed decision to consent to medical treatment or to withhold his or her consent and seek other treatment if the patient does not want genetic material to be collected).}
\end{itemize}
used from subjects in a different research study, the “participants” are often unaware of how their information is being used or where their information is located. A centralized repository system (such as the Initiative) that mandates notice be given to the government when there is any use of this sort of information, and that gives proper notice to the users, could help alleviate this concern; the basic logistics of this idea will be discussed more in the conclusion.

These are not the only concerns; in private law, contractual limitations can and do exist on the disclosure of information, such as non-disclosure agreements or material-transfer agreements. The law governing both of these would be the contractual agreements between the parties, and the privacy clauses and use restrictions would likely be material conditions to the contract. To resolve contract disputes, one must turn to economic arguments like efficient breach, which results in optimal obligations for all parties involved. If consent to use genetic information existed under an efficient breach system,


134. See infra Part III.


136. See Thomas Margoni, The Roles of Material Transfer Agreements in Genetics Databases and Bio-Banks, in COMPARATIVE ISSUES IN THE GOVERNANCE OF RESEARCH BIOBANKS 231, 231–32 (Giovanni Pascuzzi et al. eds., 2013) (“The exchange of biological and research materials is becoming more and more formalized, and—differently from a few years ago—providing institutions now tend to impose the use of specific contract forms that detail the rights and obligations attached to the material. Such contractual agreements are commonly referred to as ‘Material Transfer Agreements’, or MTAs.”).


and if a central reporting database were available, it would simplify the process of identifying the parties involved, thereby streamlining the removal of information, and, subsequently, returning the parties to a position where they would have been had the contract not been performed. Efficient breach would also return the benefits conferred or consideration (If there are any) to the researcher and by removing the information of the participants, research would incorporate a less exploitative model of consent and participation, and thereby, avoid more of the aforementioned historical\textsuperscript{139} or bioethical problems.\textsuperscript{140}

Even if one does not agree with using contract law to govern informed consent in a biobank based on efficiency grounds, there are also consumer protection reasons for supporting contract-based regulation. Current biobank databases use broad consent,\textsuperscript{141} which presumes any future researcher and future research has already been consented to, by moving to contract-based regulation of evolving consent, this model would incorporate the “opt-in” model of participation as compared to the current “opt-out” model.\textsuperscript{142} In an opt-in system, concerned participants can have a more meaningful choice regarding the use of their information,\textsuperscript{143} and it is possible researchers may maintain similar levels of participation. As a result, these alterations could address privacy concerns while leaving the system relatively intact.

\begin{itemize}
\item \textsuperscript{139} See supra notes 23–79 and accompanying text.
\item \textsuperscript{140} See supra notes 81–108 and accompanying text.
\item \textsuperscript{141} Steinsbekk, Myskja & Solberg, supra note 82.
\item \textsuperscript{142} For a description of opt-out versus opt-in in the context of becoming an organ donor, see Richard Thaler, \textit{Opt In vs. Opting Out}, N.Y. TIMES (Sept. 26, 2009), http://www.nytimes.com/2009/09/27/business/economy/27view.html (“Most states, as well as many other countries, use an ‘opt in’ or ‘explicit consent’ rule, meaning that people must take a concrete action, like going to a public library or requesting and mailing in a form, to declare they want to be [organ] donors. But many who are willing . . . never get around to such steps. An alternative approach, used in several European countries, is an ‘opt out’ rule, often called ‘presumed consent,’ in which citizens are presumed to be consenting donors unless they act to register their unwillingness. In the world of traditional economics, it shouldn’t matter whether you use an opt-in or opt-out system . . . . But many findings of behavioral economics show that tiny disparities in such rules can make a big difference. By comparing the consent rates in European countries, . . . psychologists . . . have shown that the choice of opting in or opting out is a major factor.”).
\end{itemize}
B. FEDERAL & STATE REPORTING SYSTEMS INVOLVING EVIDENTIARY COLLECTION (CRIMINAL ISSUES)

In 2013, the U.S. Supreme Court considered the constitutionality of certain police practices that routinely compare suspect biosamples to DNA databases in *Maryland v. King*.¹⁴⁴ In *King*, almost six years after an unsolved case where a woman was anonymously raped and robbed, Alonzo King was arrested for second-degree assault in a wholly separate case.¹⁴⁵ During King’s arrest, police collected a DNA sample with a cheek swab, which occurs under a Maryland law allowing for warrantless DNA collection from anyone arrested of certain felony offenses.¹⁴⁶ King’s DNA matched DNA collected from the earlier unsolved rape, and King was tried, convicted, and sentenced to life in prison for that crime.¹⁴⁷ The majority held that the statute allowing police to take a DNA swab from anyone they arrest for a serious crime did not violate the Fourth Amendment.¹⁴⁸ Thus, through the DNA collection protocol allowing for storage of information in a repository for a seemingly infinite time period, arrested persons (supposedly innocent until proven guilty) are being genetically searched for evidence they are connected to any past unsolved crimes.¹⁴⁹ The Supreme Court held that this practice was not a violation of the Fourth Amendment as it was reasonably tailored to the police investigation activities, and in doing so, the Court endorsed a practice now followed by more than half the states and federal government.¹⁵⁰

---

¹⁴⁵. *Id.* at 1965–66.
¹⁴⁶. *Id.*
¹⁴⁷. *Id.*
¹⁴⁸. *Id.* at 1980.
¹⁴⁹. *See Id.* at 1986 (Scalia, J., dissenting) (“DNA testing does not even begin until after arraignment and bail decisions are already made. The samples sit in storage for months, and take weeks to test. When they are tested, they are checked against the Unsolved Crimes Collection — rather than the Convict and Arrestee Collection . . . . The Act . . . prescribes as its purpose what our suspicionless-search cases forbid (‘official investigation into a crime’).”).
¹⁵⁰. *Id.* at 1968 (majority opinion) (“All 50 States require the collection of DNA from felony convicts . . . . Twenty-eight States and the Federal Government have adopted laws similar to the Maryland Act authorizing the collection of DNA from some or all arrestees. Although those statutes vary in their particulars, such as what charges require a DNA sample, their similarity means that this case implicates more than the specific Maryland law. At issue is a
Before King, many have argued that these systems represent a wholly unconstitutional practice. While now constitutional, DNA repositories of this magnitude fostered nearly unlimited power, and have fundamentally changed the entire manner of criminal convictions and evidentiary collection processes. Almost half the U.S. Supreme Court explicitly recognized this issue. In a dissent, Justice Scalia (joined by Justices Ginsburg, Sotomayor, and Kagan) stated:

Make no mistake about it: As an entirely predictable consequence of today’s decision, your DNA can be taken and entered into a national DNA database if you are ever arrested, rightly or wrongly, and for whatever reason.

Today’s judgment will, to be sure, have the beneficial effect of solving more crimes; then again, so would the taking of DNA samples from anyone who flies on an airplane (surely the Transportation Security Administration needs to know the “identity” of the flying public), applies for a driver’s license, or attends a public school. Perhaps the construction of such a genetic panopticon is wise. But I doubt that

standard, expanding technology already in widespread use throughout the Nation.” (citation omitted)).

151. Aaron B. Chapin, Note, Arresting DNA: Privacy Expectations of Free Citizens Versus Post-Convicted Persons and the Unconstitutionality of DNA Dragnets, 89 MINN. L. REV. 1842, 1856 (2005) (“DNA acts push the boundaries of constitutionality and survive primarily because of the status of the individual as a post-convicted person. When individuals subjected to testing do not have diminished privacy expectations, as in the context of DNA dragnets, the government interest in compelling DNA collection fails to outweigh the intrusion upon the individual under the reasonableness balancing test. Without a non-law enforcement purpose in collecting DNA in mass sweeps, the ‘special needs’ exception does not apply. Nor can a DNA sample be compelled as part of an investigatory stop, because the seizure of DNA falls outside the scope of the Terry stop-and-frisk exception. The only way to obtain a DNA sample from a nonsuspect, free citizen is through consent, but the very purpose behind the DNA dragnet may make voluntary consent practically impossible. Therefore, DNA searches of free citizens without individualized suspicion are unconstitutional.”).

152. Yale H. Yee, Criminal DNA Data Banks: Revolution for Law Enforcement or Threat to Individual Privacy?, 22 AM. J. CRIM. L. 461, 489 (1995) (“However, such data banks pose numerous problems in the realm of individual privacy. Although the bare fingerprint may not contain significant genetic information, a great danger exists in the storage of blood or saliva samples. Unauthorized access to these samples can result in serious breaches of individual privacy. Current DNA technology applied to analysis of such samples can yield a wealth of information about an individual which may serve as the basis for genetic discrimination by insurance companies, employers, or education facilities, and pose the threat of stigmatization or adverse emotional consequences. Procedural safeguards can be set in place that will adequately protect against potential breaches of privacy.”).
the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.153

As a result, it is uncontested that these new police search powers protected in King hold vast potential and controversial outcomes.154

Historically, certain individual rights and privileges protected by the constitution and granted by federal and state law are removed when a person has been convicted of a felony conviction, including: disbarment or engaging in a business relationship with the government,155 voting rights and jury service,156 firearm ownership,157 serving in the armed forces,158 flying aircraft,159 holding private radio licenses,160 holding other Federal Licenses,161 holding federal offices,162 receiving fed-

154. Chapin, supra note 151.
157. See 18 U.S.C. § 922(d)(1), (g) (2012) (preventing a person with a felony record from buying, receiving, transporting, or possessing any firearm or ammunition).
159. See 49 U.S.C. §§ 44703, 44101–44103, 44106, 44703(e), 44709, 44710 (2012) (restricting the ability to receive or renew a pilot’s license or aircraft registration for felony convictions over controlled substances).
eral employment, and receiving federal benefits among other things. This said, is the loss of genetic data privacy rights akin to these rights and is the commission of a crime sufficient to surrender this “unlimited” knowledge repository to government?

Some commentators have categorized privacy concerns with criminal justice and DNA repositories to occur in two primary instances. First, there is a “governmental intrusion, both physical and psychological,” when DNA is collected, used, and stored in a database; an intrusion that is compounded when it occurs multiple times without the individual’s knowledge or consent. Second, the government’s potentially perpetual retention of a biological sample, marks an intrusion, as the sample holds an incalculable reservoir of personal information about both the individual and the individual’s family. Are these programs narrowly tailored to sufficiently fulfill the bioethical considerations, or are these disclosures beginning to branch into the historical controversies DNA has previously faced?

C. FEDERAL CREATION OF CODIS

To better understand the implications of genetic surveillance in a civil context, we must first look to the history of ge-

162. See U.S. CONST. art. I, § 3 (providing for removal and “disqualification to hold . . . any Office of honor, Trust or Profit” upon impeachment of an official by the Senate); U.S. CONST. art. II, § 4 (providing for removal from office of the “President, Vice President and all civil Officers” upon impeachment for “Treason, Bribery, or other high Crimes and Misdemeanors”).


165. See generally Yee, supra note 152.


167. Id.


169. See supra notes 90–93 and accompanying text.

170. See supra notes 23–64 and accompanying text.
metic surveillance by the Federal Bureau of Investigation (FBI). Central to Maryland v. King is the FBI’s use of a DNA repository system. The FBI does the criminal investigation for the federal government, and is housed in the Department of Justice. The mission statement of the FBI states:

[a]s an intelligence-driven and a threat-focused national security organization with both intelligence and law enforcement responsibilities, the mission of the FBI is to protect and defend the United States against terrorist and foreign intelligence threats, to uphold and enforce the criminal laws of the United States, and to provide leadership and criminal justice services to federal, state, municipal, and international agencies and partners.

The FBI is charged with “gathering and reporting facts, locating witnesses, and compiling evidence in cases involving Federal jurisdiction . . . provid[ing] law enforcement leadership and assistance to State and international law enforcement agencies.” The Bureau’s role is to investigate all violations of federal law except those legislatively or otherwise delegated to another agency.

The Combined DNA Index System (CODIS) began in 1990 as a pilot project by the FBI in conjunction with fourteen state and local laboratories. CODIS and National DNA Index System (NDIS) were both officially established in 1998 following the passage of the DNA Identification Act of 1994 by Congress. The legislative authorization of CODIS required the FBI to establish quality assurance standards ensuring that DNA records were treated with integrity when being entered into the system and that strict limitations were placed on the data that could be entered into CODIS and how that data could

---

174. See Federal Bureau of Investigation, supra note 172.
175. Id.
subsequently be used. \cite{office_of_the_inspector_gen__dept_of_justice_audit_report__2001} CODIS generally uses Rapid DNA, or Rapid DNA Analysis, which is the process for creating a CODIS Core Short Tandem Repeat (STR) profile from a cheek swab sample via fully automated “extraction, amplification, separation, detection and allele calling.” \cite{rapid dna_or_rapid dna_analysis__2015} As of 2006, CODIS contained over 3.3 million DNA profiles of convicted offenders, over 142,000 DNA profiles from crime scenes, and the system has produced 36,000 matches to previously unsolved crimes in forty-nine states. \cite{dale_et_al__2015} As there is no “formal interface between CODIS and any criminal history record information systems,” CODIS does not “include any personally identifying information about the subject of the DNA sample.” \cite{dale_et_al__2015} In general, states have followed the federal database architecture and have not added personally identifying information, with some states expressly prohibiting any connections between criminal history record information and DNA profiles. \cite{dal_2015}

Looking to the administrative structure of the program, the Department of Justice houses CODIS, which, in turn, has the NDIS, which, in turn, houses the Rapid DNA Index System (RDIS). \cite{rapid dna__2001} At the FBI, the Rapid DNA Program Office directs “the development and integration of Rapid DNA technology for use by law enforcement.” \cite{rapid dna__2001} Essentially, all federal agencies, state and local agencies have access to the system. Further, the FBI has fully integrated the system to be capable of performing cheek swab STR analysis in one to two hours and “initiating DNA enrollment and searches from a police booking station.” \cite{rapid dna__2001}

This system allows for police to match cheek swaps against a

\begin{thebibliography}{99}
\bibitem{dale_et_al__2015} Dale et al., supra note 176.
\bibitem{dal_2015} Id. at 1.
\bibitem{dal_2015} Id.
\bibitem{rapid dna__2001} Rapid DNA, supra note 179.
\bibitem{rapid dna__2001} Id. (“The Program Office works with the Department of Defense, the Department of Homeland Security, the National Institute of Standards and Technology, the National Institute of Justice, and other federal agencies to ensure the coordinated development of this new technology among federal agencies. The Program Office also works with state and local law enforcement agencies and state bureaus of identification . . . to facilitate the effective and efficient integration of Rapid DNA [in the state criminal justice system].”).
\bibitem{rapid dna__2001} Id.
\end{thebibliography}
national index. However, the FBI states that it makes minimal use of Rapid DNA on crime scene samples:

At this time, these [the FBI’s] goals do not include the use of Rapid DNA technology on crime scene (forensic) samples because of the differences between forensic and known reference (offender/arrestee) samples. These differences may include the nature or type of sample, typical sample quantity and potential for reanalysis. A forensic sample may not be amenable to fully automated processing due to limitations in its quality and quantity.

In conflict with this statement of the bureau’s goals is the creation of forensic sample databases.

In its original form, CODIS consisted of two indices: the Forensic Index and the Convicted Offender Index. The Forensic Index contains evidentiary profiles developed from biological material such as semen, saliva, or blood found at crime scenes. The Convicted Offender Index contains profiles of individuals convicted of crimes specified by State laws. All 50 states have passed DNA legislation authorizing the collection of DNA profiles from certain convicted offenders for submission to CODIS. In recent years, CODIS has added new indices; including the Arrestee Index, the Missing or Unidentified Persons Index, and the Missing Persons Reference Index. CODIS automatically searches across these indices for a potential match to aid criminal investigations of crimes for which unknown biological evidence has been recovered.

When a “hit” (or positive match) “is obtained from a convicted offender or arrestee sample,” the hit is typically viewed as probable cause, thereby allowing for the government to take additional DNA sample(s) from the suspect for confirmatory purposes by the laboratory. Thus, some have speculated the system bypasses the Fourth Amendment’s mandate of a warrant for a reasonable search or seizure.

While the idea of CODIS might be problematic in the abstract, the system’s actual implementation and management have attracted significant detractors and proven to be rife with conflicts. The actual operation of the system may extend be-

186. Id.
187. Id.
189. Id.
190. See Chapin, supra note 151.
yond the intended statutory authority provided by the DNA Identification Act of 1994. The management of the database is a cause of concern because the accuracy of decisions made off the database have significant impacts on people’s lives. An audit by the Department of Justice found that the FBI implemented CODIS (and companion program(s)) nationwide, but largely failed to conduct mandatory monitoring of program accountability—of the “eight state and local laboratories disclosed” in the audit, “four laboratories did not fully comply with the FBI’s quality assurance standards and national index requirements.” These laboratories subsequently agreed to perform corrective actions to resolve operational deficits, yet it remains the case that 50% of laboratories audited were out of compliance. More troubling, the labs had been required for years prior to have annual audits for quality assurance, but labs were not reporting audit results to the FBI and instead “the laboratories contributing DNA profiles to the national index simply certified that they had been audited and that they were in compliance with the legislation and quality assurance standards.”

Access to identifiable information in the CODIS database is highly restricted and limited by physical and administrative barriers. “Access to these computers is limited to only those

implementation, such as the widespread practice of investigating “partial matches” who are likely relatives to some degree of the perpetrator and now “guilt[y] by genetic association,” and the FBI’s obstruction of external reviews of the false positive rate for matches given current cutoffs and practices on the number of allele’s and locations that must align before a profile is considered a match).

193. OFFICE OF THE INSPECTOR GEN., supra note 178, at iii.
194. Id.
195. Id. at ii–iii.
196. Frequently Asked Questions (FAQs) on the CODIS Program and the National DNA Index System, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/lab/biometric-analysis/codis/codis-and-ndis-factsheet (last visited Feb. 9, 2015) (“The computer terminals/servers containing the CODIS software are located in physically secure space at a criminal justice agency. Access to these computers is limited to only those individuals authorized to use CODIS and approved by the FBI. Communications between participating federal, state, and local laboratories occur over a wide area network accessible to only criminal justice agencies approved by the FBI. Pursuant to federal law (the DNA Identification Act of 1994), DNA data is confidential. Access is restricted to criminal justice agencies for law enforcement identification purposes. Defendants are also permitted access to the samples and anal-
individuals authorized to use CODIS and approved by the FBI.”197 However, as soon as information is de-identified, it can be used by authorized entities for “research and protocol development purposes.”198 Thus, pursuant to the DNA Identification Act of 1994199 and the Freedom of Information Act,200 these data can be divulged to approved researchers; it is unclear if the Initiative will have access to this information.

D. FREEDOM OF INFORMATION ACT

The Freedom of Information Act (FOIA) gives citizens a right to access the federal government’s information.201 Specifically, the act provides a right to access federal agency records, unless the records are subject to any of nine exemptions that allow denial of the request or redaction of exempt portions of the record.202 A FOIA request can be made for any agency record.203 Federal agencies (including the FBI and NIH204) are re-

yses performed in connection with their cases. If all personally identifiable information is removed, DNA profile information may be accessed by criminal justice agencies for a population statistics database, for identification research and protocol development purposes, or for quality control purposes. The unauthorized disclosure of DNA data in the National DNA database is subject to a criminal penalty not to exceed $250,000.”.

197. Id.
198. Id.
199. Id. (“The DNA Identification Act of 1994 (42 U.S.C. §14132) authorized the establishment of this National DNA Index. The DNA Act specifies the categories of data that may be maintained in NDIS (convicted offenders, arrestees, legal, detainees, forensic (casework), unidentified human remains, missing persons and relatives of missing persons) as well as requirements for participating laboratories relating to quality assurance, privacy and expungement.”).
200. See infra notes 201–21 and accompanying text.
202. 5 U.S.C. § 552(a)(2), (a)(3) (2012) (requiring that each agency to “promptly” “make available for public inspection and copying” “all records, regardless of form or format”); 5 U.S.C. § 552(b)(1)–(9) (listing exemptions to FOIA production, including exemption (b)(6) for “medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy” and exemption (b)(7) for “records or information compiled for law enforcement purposes, but only to the extent that the production” would interfere with a proceeding, deprive a person of rights, constitute an invasion of privacy, discloses a confidential source, discloses a law enforcement technique, or endangers life or physical safety); see also What is FOIA?, U.S. DEPT OF JUSTICE, http://www.foia.gov/about.html (last visited Feb. 9, 2015).
required to have distinct systems for production of information requested under FOIA.205

Since there are different state laws regarding health privacy, there have been calls for a single, uniform, comprehensive set of federal laws to govern health privacy.206 Congress has been unable to pass such federal legislation,207 although HIPAA and GINA now prevent some of the more egregious violations of medical privacy, and the privacy provisions of the Health Information Technology for Economic and Clinical Health (HITECH) Act extend HIPAA restrictions to the "business associates of a covered entity."208 The Privacy Act of 1974 regulates how federal agencies disseminate personal information.209 Federal agencies use these FOIA exceptions to resist

204. Requesting FBI Records, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/foia/requesting-fbi-records (last visited Feb. 9, 2015) ("The Freedom of Information Act allows any person—except fugitives, federal agencies, and foreign intelligence agencies—to request information about organizations, businesses, investigations, historical events, incidents, groups, or deceased persons."); Freedom of Information Act Office, NAT'L INST. OF HEALTH, http://www.nih.gov/odu/foia/ (last modified Oct. 6, 2015) ("The NIH FOIA office generally handles three different categories of requests: requests for information maintained by the Office of the Director, NIH requests that involve trans NIH issues or initiatives unless a specific IC has responsibility, requests for information that will not be released because it is protected by one or more of the FOIA’s nine exemptions or three exclusions").

205. 5 U.S.C. § 552(a)(1)(A)–(E) (requiring each agency to publish regulations to offer guidance to the public on how requests are handled, and rules of procedure for making and fulfilling requests).

206. See generally THE CTR. FOR PUB. INTEGRITY, NOTHING SACRED: THE POLITICS OF PRIVACY 26–28 (1998) (describing cases of employees being fired based on health records, and disclosures of health status and history by hospital workers in the years before some protections were created by HIPAA and GINA); Charity Scott, Is Too Much Privacy Bad for Your Health? An Introduction to the Law, Ethics, and HIPAA Rule on Medical Privacy, 17 GA. ST. U.L. REV. 481, 508 (2000) (same).

207. See THE CTR. FOR PUB. INTEGRITY, supra note 206; Scott, supra note 206.


209. 5 U.S.C. § 552a(b) ("No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains . . . ."); see Scott, supra note 206.
disclosure of personal information including health data and patient research records.210

This said, researchers are not bound to the same laws the physicians or covered health services organizations are.211 Specifically, “existing regulation of biomedical research . . . occurs at two levels.”212 First, federal law “requires researchers to submit proposals for studies of human subjects to expert panels, which must judge those proposals based on adherence to federal regulations for the protection of human subjects,” and, second, the individual research subjects must “be fully informed about the nature, scope, and risks of the research and agree formally to participate in it.”213 These requirements are spelled out in the Federal Research Regulations.214 That said, subsequent use of these data sets, where participants have given no consent, runs rampant in medical research.215 Further, case law has shown that there is no private cause of action under the federal research regulations.216 Consumer advocacy groups urged Congress to adopt laws mandating that research using medical records undergo IRB-like review allowing researchers to proceed without express informed consent only if consent were impracticable and if confidentiality safeguards were in place.217 Yet health plans and pharmacies have objected, claiming such procedures would impose confidentiality duties (and estimated high costs) beyond traditional scientific research projects into routine health care operations “such as outcome research, disease management programs, or other activities aimed at improving the quality of care.”218

210. See Scott, supra note 206.
212. Id. at 1399.
213. Id. at 1399–400.
215. See generally Tilousi v. Ariz. State Univ. Bd. of Regents, No. 04-CV-1290, 2005 WL 6199562, at *2 (“As to plaintiffs’ [research participants] claim that they had a fiduciary relationship with all defendants [genetic researchers], plaintiffs allege no facts sufficient to establish such a relationship. As defendants point out, plaintiffs do not even allege that any of the defendants accepted the trust and confidence of plaintiffs, but instead plaintiffs’ allegations focus on [their reliance on the first researcher].”).
216. ANDREWS, MEHLMAN & ROTHSTEIN supra note 23, at 155.
217. Scott, supra note 206, at 518 (describing advocacy efforts to pass privacy protections in the 1990’s prior to the HIPAA Privacy Rule).
Alternatively, those restrictions and protocols on data sharing often do not apply in the criminal context, where the FBI operates under a much different paradigm.\textsuperscript{219} Currently, HIPAA allows officers to gain access to medical records without obtaining of a search warrant or even notice to patients.\textsuperscript{220} Consumer groups and civil rights organizations have advocated for new federal privacy laws to create tougher standards before law enforcement officers could get medical records, but no substantial changes have occurred.\textsuperscript{221}

\begin{flushleft}
\par
\textsuperscript{219} See Scott, supra note 206, at 520.
\textsuperscript{220} 45 C.F.R. § 164.512(f); \textit{FAQ on Government Access to Medical Records}, ACLU [hereinafter \textit{FAQ on Government Access}], https://www.aclu.org/faq-government-access-medical-records?redirect=technology-and-liberty/faq-government-access-medical-records (last visited Oct. 16, 2015) (“The HIPAA rules provide a wide variety of circumstances under which medical information can be disclosed for law enforcement-related purposes without explicitly requiring a warrant. These circumstances include (1) . . . requests for information to identify or locate a suspect, fugitive, witness, or missing person (2) instances where there has been a crime committed on the premises of the covered entity, and (3) in a medical emergency in connection with a crime. In other words, law enforcement is entitled to your records simply by asserting that you are a suspect or the victim of a crime . . . . Section 215 of the Patriot Act allows the FBI Director or his designee to get a court order . . . requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution. This power appears to apply to medical records.”).
\textsuperscript{221} \textit{FAQ on Government Access}, supra note 220 (“The ACLU believes that this easy, warrantless access to our medical information violates the U.S. Constitution, especially the Fourth Amendment, which generally bars the government from engaging in unreasonable searches and seizures. However, because the Patriot Act and the HIPAA regulations have only recently gone into effect, their constitutionality remains largely untested, although at least one legal challenge to the HIPAA rules is underway, and more challenges are likely.”); see, e.g., \textit{Medical Records Confidentiality in a Changing Health Care Environment: Hearing on S. 881 and S. 578 Before the S. Comm. on Health, Education, Labor, and Pensions}, 106th Cong. 1 (1999) (statement of Ronald H. Weich, legislative consultant, Am. Civil Liberties Union); Alissa J. Rubin, \textit{Privacy Initiatives Elicits Praise, Concern}, L.A. TIMES, Oct. 30, 1999, at A12; Scott, supra note 206.
\end{flushleft}
E. EUROPEAN “RIGHT TO BE FORGOTTEN”

1. History of the Right to be Forgotten

European Union Directive 95/46/EC was issued in 1995.222 This directive did not explicitly outline the current “right to be forgotten.”223 When it was issued, Article 12 of the Directive 95/46/EC, the EU gave a legal basis, however not explicit privacy, for internet protection for individuals.224 Specifically, it describes the ability for individuals to “determine the development of their life in an autonomous way, without being perpetually or periodically stigmatized as a consequence of a specific action performed in the past.”225 As suggested, this is a derivation “from a right, originally accorded to criminals who had served time, to have their records expunged so that they’re able to start life over;” the this right is premised on the policy of rehabilitation.226 In Europe, though, this “right to be forgotten” has extended beyond solely the criminal sphere and into a general concern that includes even civil matters in cyberspace, and acknowledges that without such a right, humans may “never grow past the moment of our greatest humiliation.”227

The right was articulated and generalized in EU case law in 2014, in Google Spain v. Gonzalez.228 In this case, a resident of Spain, Mario Costeja Gonzalez, filed a complaint against La Vanguardia Ediciones SL (the publisher of a daily newspaper with a large circulation in Spain . . .) and against Google Spain and Google Inc . . . contending that, when an internet user entered his name in the search engine of the Google group (‘Google Search’), the list of results would display links to two pages of La Vanguardia’s newspaper, of January and March 1998. Those


223. European Commission, supra note 222.


225. Id. at 230.

226. Williams, supra note 3.

227. Id.

pages . . . contained an announcement for a real-estate auction organ-
ised following attachment proceedings for the recovery of social secu-
ricy debts owed by . . . Gonzalez.229

First, González requested
that La Vanguardia be required either to remove or alter those pages
so that the personal data relating to him no longer appeared or to use
certain tools made available by search engines in order to protect the
data. Second, he requested that Google Spain or Google Inc. be re-
quired to remove or conceal the personal data relating to him so that
they ceased to be included in the search results and . . . in the links to
La Vanguardia.230

He argued “that the attachment proceedings concerning him
had been fully resolved for a number of years” and now were
irrelevant.231 The European Court found that search engines
like Google must remove information that is “inadequate, irre-
levant or no longer relevant” when a member of the public so
requests.232 “The ruling seems broad enough to apply to re-
solved debts, revenge porn, indeed any information that affects
people’s honor, dignity or privacy.”233

2. The “Right to Be Forgotten” and the Precision Medicine
Initiative

Perhaps the most difficult area of discussion revolving
around a “right to be forgotten” is what the right would actual-
ly entail and what this even means; some claim this right’s
ambiguity would cause more problems as opposed to presenting
solutions.234 In the context of genetic information and the Pre-
cision Medicine Initiative, the right to be forgotten would entail
an individual’s ability to withdrawn their genetic information
from research uses. Such a right is needed as a solution to
many of the difficult issues the medical research community
has faced with informed consent, which will only become ampli-
fied in a big data world.

229. Court of Justice of the European Union, supra note 222.
231. Id.
232. Id. ¶ 93.
233. Williams, supra note 3.
234. See Luciano Floridi, Right to Be Forgotten Poses More Questions than
Answers, GUARDIAN (Nov. 11, 2014, 5:54 AM), http://www.theguardian.com/technology/2014/nov/11/right-to-be-forgotten-
more-questions-than-answers-google (noting the potential problems as dis-
cussed at a Google advisory council meeting).
[F]or better or worse, the Internet has become a sort of historical record, and search engines are its indispensable catalog...

Some of the best features of the Internet — the vast amount of information it makes available, its openness, its ability to connect users around the globe — are also the ones that conflict most sharply with individual privacy. Once information posted online, words and images can be duplicated so rapidly and preserved so cheaply that they become nearly impossible to erase.235

In the context of genetic information, and specifically this massive database to be compiled by NIH, this would suggest far-reaching, nearly endless possibility for information use that would bypass the protections of HIPAA and GINA regulations.

With genetics, the problem is much larger than simply misinformation, like that suffered in the Google Spain case. First, since the data processed from various individuals would have been authorized (or forfeited) in previous research contexts, the consents and authorizations from the earlier studies may be legally sufficient for inclusion in the new database—meaning an individual that provided broad consent for use of their samples previously may not know how widely their samples are eventually used.236 Although Department of Health and Human Services regulations require authorization or waiver from the individual to the extent their protected health information would be involved in “the development of research repositories and databases for future research purposes,” there are data sets where existing, broadly-given research authorizations would not need an individual’s new consent, and even when it would be needed, an IRB panel could waive the requirement.237


236. See FOLEY & LARDNER LLP, PRIVACY ISSUES IN THE SHARING OF GENETIC INFORMATION 2–3 (2014), http://www.personalizedmedicinebulletin.com/wp-content/uploads/sites/205/2014/09/PrivacyIssuesintheSharingofGeneticInformation.pdf (describing situations where “a covered entity” would be permitted “to use and disclose PHI [protected health information] for research purposes, without an individual’s authorization,” including when broad consent was given even for unknown future uses, and when an IRB panel determines a waiver for individual authorization is permissible (footnotes omitted)).

237. Id. (“An IRB operating under a federal-wide assurance or a privacy board that functions under the Privacy Rule may grant a waiver or alteration of written authorization if the proposed use or disclosure will pose minimal risk to participants’ privacy, the research could not practicably be conducted.
Second, “[c]ollection and use of a limited data set (which may include geographic information other than street address, all elements of dates and ages, and certain other unique identifying characteristics or codes)” is allowed. This type of mostly de-identified data is still regulated and would require users to sign data use contracts assuring that no attempt to re-identify the dataset will be made. NIH currently controls access to genetic information by encouraging researchers to use only these partially de-identified datasets; but identity tracking attacks have been shown to be capable of re-identifying about sixty percent of people in the U.S. based on only birth date, sex, and zip code, while attacks using even partial genetic information can allow identification without geographic or personal metadata. However, de-identified data is not protected health information under HIPAA, so it is not regulated by HIPAA or subject to its protections. At that point, the traditional bounds of information privacy protections no longer have teeth, however, in a world of big data, what might be considered de-identified to meet HIPAA requirements, may still be re-identified given the amount of information available on the internet. In NIH draft documents concerning how to handle privacy concerns, advisors seem to both acknowledge these complexities, but nonetheless believe that restrictions in data use contracts will be adequate.

without the waiver or alteration of authorization and cannot be conducted using de-identified information, and other specified criteria are met.”).

238. Id.
239. Id. at 3 (“A Covered entity may release a limited data set if the researcher signs a data use agreement (DUA), which assures the Covered entity that the recipient will protect the limited data set and will not make any effort to re-identify individuals using the data set.”).
241. See FOLEY & LARDNER LLP, supra note 236.
242. Erlich & Narayanan, supra note 105, at 410–16 (describing different types of identity tracing attacks that can be used to re-identify individuals in de-identified DNA data sets).
243. PRECISION MEDICINE INITIATIVE (PMI) WORKING GROUP, THE PRECISION MEDICINE INITIATIVE COHORT PROGRAM – BUILDING A RESEARCH FOUNDATION FOR 21ST CENTURY MEDICINE 72 (2015), http://acd.od.nih.gov/reports/DRAFT-PMI-WG-Report-9-11-2015-508.pdf (“[T]he proliferation of data mining methods and potential naming sources (voter lists, public registries, social media postings, ancestry web sites, etc.) means that technology alone will be insufficient to address issues of data privacy for the PMI cohort . . . Acceptable use policies with substantial enforceable sanctions will need to be developed or adapted from other similar research efforts . . .”).
What is proposed as a solution here? Simply, a method of removal of this information from the database, and a right to remove subsequent links to this data from publically available sources of this information including government publications and search engines. The management of this right may need to differ between civil and criminal contexts; however, a mechanism needs to be in place in order to limit the disclosure of this vast array of information as this information stretches far beyond the traditional bounds of freedom of speech.244

Some argue there are massive problems with this sort of approach, and believe it leaves critical unresolved flaws, including: creating a two-tiered approach to information without a way to deal with information categorization; creating a pseudo-territoriality of the law that conflicts with the non-territoriality of the internet; creating a conflict between the “right to be forgotten” and the “right to information” which are both proxies of protected privacy rights; how to delineate “relevance” of personal information independent of the purpose for seeking the information; and the conflict between “public interest” and “what is interesting to the public.”245 Not all of these concerns can be addressed in the conclusion of this note (as there is no federal right proposed), however some general aspects of these concerns can be addressed.

3. Why Not Expungement?

Some would claim that expungement proceedings246 could be used to remove genetic information from databases, and

---


would rectify problems arising from extended use of genetic information without creating conflicts with First Amendment protections. However, expungement remedies are generally only allotted to those who have been through criminal proceedings. Further, expungement proceedings fail to recognize that the nature, quality, quantity, and historical and sociocultural context that genetic information contains makes any full recovery from past disclosure impossible. Further, expungement remedies are extremely limited to state statutes; the Second Circuit posited that when looking at expungement proceedings, the law “only requires that certain official records be erased. The few enumerated exceptions to the erasure requirements . . . confirm that the legislature contemplated erasure only in the context of the judicial and law enforcement systems.” However, even if an individual is entitled to an

going to court to ask a judge to seal a court record. It is important to remember that an expunged record is NOT destroyed. The police, FBI, immigration officers, and other public officials may still see sealed court files for certain purposes. Usually, people ask for an expungement when they have been denied a job, housing, or a professional license because of their criminal background.

247. For examples of courts balancing the First Amendment and the expungement of criminal records, see, for example, G.D. v. Kenny, 15 A.3d 300, 315–16 (N.J. 2011) (“[T]he expungement statute does not transmute a once-true fact into a falsehood. It does not require the excision of records from the historical archives of newspapers or bound volumes of reported decisions or a personal diary . . . . It is not intended to create an Orwellian scheme whereby previously public information—long maintained in official records—now becomes beyond the reach of public discourse on penalty of a defamation action. Although our expungement statute generally permits a person whose record has been expunged to misrepresent his past, it does not alter the metaphysical truth of his past, nor does it impose a regime of silence on those who know the truth.”); Bahr v. Statesman Journal Co., 624 P.2d 664, 666 (Or. Ct. App. 1981) (“The expungement statute does not, however, impose any duty on members of the public who are aware of the conviction to pretend that it does not exist. In other words, the statute authorizes certain persons to misrepresent their own past. It does not make that representation true.”).

248. See Criminal Expungement, supra note 246.

249. See supra Part I.

250. Martin v. Hearst Co., 777 F.3d 536, 551 & n.4 (2d Cir. 2015) (“[F]ingerprints, pictures and descriptions and other identification data . . . are not among the records whose disclosure is governed . . . [t]he fundamental purpose of the [expungement] statute is served by permitting limited disclosure of the records to counsel for the state in order for it to take reasonable steps to defend itself against [the defendant’s] threatened action while sealing and segregating the records to prevent disclosure to anyone else.” (citations omitted)) (footnotes omitted).
expungement proceeding under state law, courts have found that news stories, now no longer relevant in the public domain, can continue to pester individuals. As a result, even if the law “permits a person whose record has been expunged to misrepresent his past,” they still have the potential for their previous misdeeds to haunt them long after serving their criminal sentences.

Actions have been taken in the United States to solve these issues. The Second Chance Act aimed to improve employment outcomes for people returning to communities after incarceration; “the legislation authorizes federal grants to government agencies and nonprofit organizations to provide support strategies and services designed to reduce recidivism by improving outcomes for people returning from prisons, jails, and juvenile facilities.” However, success rates (defined as gaining employment) have so far trailed other civilian populations, suggesting that more action is necessary.

Following the European Union’s (EU) recognition of the “right to be forgotten,” California saw the need for more action and “enacted its own version of the requirement, though lim-

251. See Adam Liptak, Expunged Criminal Records Live to Tell Tales, N.Y. TIMES (Oct. 17, 2006), http://www.nytimes.com/2006/10/17/us/17expunge.html (“In 41 states, people accused or convicted of crimes have the legal right to rewrite history. They can have their criminal records expunged, and in theory that means that all traces of their encounters with the justice system will disappear.”).


253. See, e.g., Kenny, 15 A.3d at 316.

254. Hearst Co., 777 F.3d at 553 (“Reasonable readers understand that some people who are arrested are guilty and that others are not. Reasonable readers also know that in some cases individuals who are arrested will eventually have charges against them dropped. Reporting Martin’s arrest without an update may not be as complete a story as Martin would like, but it implies nothing false about her.”).


259. CAL. BUS. & PROF. CODE §§ 22580–22581; Segalis & Ross, supra note 258.
260. Segalis & Ross, supra note 258.
261. See supra Part I.
262. Compare Peter Fleischer, Implementing a European, Not Global, Right to Be Forgotten, GOOGLE: EUR. BLOG (July 30, 2015), http://googlepolicyeurope.blogspot.com/2015/07/implementing-european-not-global-right.html (“We believe that no one country should have the authority to control what content someone in a second country can access.”), and Gabrielle Bernstein & Catherine Muyl, The Right to Be Forgotten: Another Scuffle Between Google and the French Data Protection Authority, JD SUPRA (Aug. 12, 2015), http://www.jdsupra.com/legalnews/the-right-to-be-forgotten-another-44641/ (“On 30 July 2015 Google published a post on its EU blog which they stated that they disagreed [with the international right to be forgotten] for three reasons. First, ‘while the right to be forgotten may now be the law in Europe, it is not the law globally.’ . . . Secondly, Google argued that ‘content that is declared illegal under the laws of one country, would be deemed legal in others . . . . [and] the Internet would be only as free as the world’s least free place.’ ”), with Transparency Report: European Privacy Requests for Search Removals, GOOGLE, http://www.google.com/transparencyreport/removals/europeprivacy?hl=en (last updated Oct. 12, 2015) (“Total URLs that Google has evaluated for removal: 1,162,529 URLs” as of October 2015).
tion even of embarrassing material as long as it was legally obtained.”

This said, free speech has contextual limits, but balancing rights and competing interests of privacy, surveillance, freedom of information, and censorship is not a new legal issue nor is it impossible to cure. The Second Circuit has expressly noted that facts, from a previous court process cannot be erased. But, the Supreme Court has stated that certain categories of information “implicate privacy concerns far beyond those implicated by the search of [physical effects]” when the information “differ[s] in both a quantitative and a qualita-

263. Williams, supra note 3.


266. Martin v. Hearst Co., 777 F.3d 536, 551 (2d Cir. 2015) (interpreting a Connecticut statute requiring erasure of records of an arrest if the person if found not guilty, to apply only to official judicial and law enforcement records of the arrest and not extending to other publishers or statements like testimony given in a previous court case).
tive sense,” and thereby requires extra government procedures to protect individual rights—such as, in this case, a warrant to search a cellular telephone. It is not a stretch to analogize the nature, quality, and quantity of data that is online or in a cell phone to that of DNA, as some commentators have done. Further, since expungement of DNA data may not be feasible, and since this data may not really implicate issues of the First Amendment, perhaps it is possible for a narrowly created government remedy to provide a “Right to Be Forgotten” for solely genetic information erasure.

III. CONCLUSION: POLICY CONSIDERATIONS AND MOVING FORWARD

This paper has presented the legal issues around the mass collection, storage, and use of DNA information from an array of perspectives to help illustrate the legal nuances with creating the Precision Medicine Initiative. This note now moves to rationalize how to fix them with a number of different ideas.

As a litigation strategy, courts, akin to those in the European Union, should consider more equitable remedies as valid when considering a petition for removal of DNA data. Considering that Google Spain arose from a cause of action for an injunction, and subsequently, an equitable remedy was granted, it would be logical to assume a similar cause of action and strategy could be tried for DNA-related data. Further, it may be more logical to assume that when DNA information is disclosed (unless tangible damages could be calculated or there was some element of slander, libel, or fraud), an equitable remedy would be sufficiently tailored to the various parties’ interests. Further, by omission of the expressly monetary component of this remedy, courts would forgo those who have solely financial incentives for bringing a lawsuit. Finally, allowing this express public policy rationale could incentivize both pri-
vate and public actors to follow modern principles of bioethics when dealing with personal genetic data.

As a legislative strategy, Congress should pass a law to adopt a “Right to Be Forgotten” solely for the context of DNA information. Such a right would not remove other sorts of information that could be linked back to a person, like those currently used in law enforcement to establish probable cause and allow for a warrant to be obtained to investigate newly found criminal activity.\(^{272}\) As with the Health Information Privacy Awareness Act, the Fair Credit Reporting Act, or the Genetic Information Non-Discrimination Act, Congress has shown its ability to pass a law to create a “black box” of protected information.\(^{273}\) For Genetics, it would make sense for Congress to allow a narrowly tailored, solely contextual “Right to Be Forgotten” pertaining to just DNA information. As a result, those harmed by these issues could remove any and all traces of this information, and appease those concerned with preservation of civil liberties. This process may differ depending on if the DNA was collected in a civil or criminal context; civil “forgetting” may be implemented immediately, whereas criminal “forgetting” may be subject to a more formal process of expungement and administrative review to ensure law enforcement needs are preserved. Hopefully, given the increased volume, velocity, and variety of personal data that exists, removing DNA information stored in CODIS (or other criminal databases) after a period of time (assuming a criminal investigation has been closed or after some Congressionally defined period) would be optimal. Ideally, limiting the perpetuity of stored DNA information should be possible in a way that balances civil rights to privacy and civil liberties to speak and publish information freely.

As an administrative strategy, federal agencies, like the Department of Justice or Department of Health and Human Services, should track public and private DNA data as a safeguard. In conjunction with the previous policy argument, since DNA information can be disclosed to third-parties, the federal government should manage a list that has participants’ data to decrease concerns involving improper use of DNA data. By adopting this process, the federal government could give any participant who wishes to be “forgotten,” the ability to know

\(^{272}\) See supra Section II.C.  
\(^{273}\) See, e.g., The Privacy Rule, supra note 18; Genetic Information Discrimination, supra note 19.
who to contact to remove traces of their genetic information. To make these reporting requirements work, state data collection of DNA should be reported to the federal government in order to manage and track where participants’ genetic information is located. Given their recent history of inaction, if Congress is unable to come to consensus on this right, a more narrowly tailored, administrative remedy could be crafted by the Department of Health and Human Services or Department of Justice to remove or enforce a removal of genetic information; this said, this remedy would be severely limited to the jurisdiction of these agencies.

Finally, the federal government should create a unified process to notify researchers, or other third parties using genetic information, when a former participant opts to remove their information. By having this centralized process, barriers to removing third party information will be minimized, though not completely mitigated. And by placing this burden on the government, as compared to citizens, participants will be better able to remove information, and government will be better able to police those who violate non-compliance with these policies.

Overall, the right to genetic privacy, and further, the right for a genetic “Right to Be Forgotten” offers a ripe conflict that will need to be considered soon by courts, elected officials, and public policymakers. Considering the historical turmoil over decision-making based on genetic information, modern bioethical concerns, and a myriad of privacy and genetic-specific laws orbiting the regulation of genetic information, a “Right to Be Forgotten” seems like a logical step. Further, since management of certain types of information (and especially genetic information) have been contextually limited over the course of Supreme Court jurisprudence, federal and state laws, and administrative regulations, it makes sense for the upcoming Precision Medicine Initiative to spearhead progress in addressing privacy concerns and allowing for participants to make meaningful choices regarding the use of their individual genetic information. Though ambitious, this logical conclusion would be a step in the right direction for American privacy rights.