Public Policy Considerations for Recent Re-Identification Demonstration Attacks on Genomic Data Sets: Part 1 (Re-Identification Symposium)

May 29, 2013 (https://blog.petrieflom.law.harvard.edu/2013/05/29/public-policy-considerations-for-recent-re-identification-demonstration-attacks-on-genomic-data-sets-part-1-re-identification-symposium/) mmeyer (https://blog.petrieflom.law.harvard.edu/author/mmeyer/) Genetics (https://blog.petrieflom.law.harvard.edu/category/genetics/), Health Information Technology (https://blog.petrieflom.law.harvard.edu/category/health-information-technology/), Human Subjects Research (https://blog.petrieflom.law.harvard.edu/category/human-subjects-research/), Medical Privacy (https://blog.petrieflom.law.harvard.edu/category/medical-privacy/), Re-Identification Symposium (https://blog.petrieflom.law.harvard.edu/category/blog-symposia/re-identification-symposium/)

By Michelle Meyer (https://blogs.harvard.edu/billofhealth/author/mmeyer/)

This post is part of *Bill of Health*'s symposium on the Law, Ethics, and Science and Re-Identification Demonstrations. We'll have more contributions throughout the week. Background on the symposium is here (https://blogs.law.harvard.edu/billofhealth/2013/05/13/online-symposium-on-the-law-ethics-science-of-re-identification-demonstrations/). You can call up all of the symposium contributions by clicking here (https://blogs.law.harvard.edu/billofhealth/category/re-identification-symposium/). —MM

(https://i0.wp.com/petrieflom.wpengine.com/wp-content/uploads/2013/05/dan.jpg?ssl=1)Daniel C. Barth-Jones, M.P.H., Ph.D. (https://www.mailman.columbia.edu/our-faculty/profile?uni=db2431), is a HIV and Infectious Disease Epidemiologist. His work in the area of statistical disclosure control and implementation under the HIPAA Privacy Rule provisions for de-identification is focused on the importance of properly balancing competing goals of protecting patient privacy and preserving the accuracy of scientific research and statistical analyses conducted with de-identified data. You can follow him on Twitter at @dbarthjones (https://twitter.com/dbarthjones).

Re-identification Rain-makers

The media's "re-identification rain-makers" have been hard at work in 2013 ceremoniously drumming up the latest anxiety-inducing media storms. In January, a new re-identification attack providing "surname inferences" from genomic data was unveiled and the popular press and bloggers thundered, rattled and raged with headlines ranging from the more staid and trusted voices of major newspapers (like the *Wall Street Journal*'s: "A Little Digging Unmasks DNA Donor Names. Experts Identify People by Matching Y-Chromosome Markers to Genealogy Sites, Obits; Researchers' Privacy Promises 'Empty' (https://online.wsj.com/article/SB10001424127887323783704578247842499724794.html)") to near "the-sky-is-falling" hysteria in the blogosphere where headlines screamed: "Your Biggest Genetic Secrets Can Now Be Hacked, Stolen, and Used for Target Marketing (https://io9.com/5976845/your-biggest-genetic-secrets-can-now-be-hacked-stolen-and-used-for-target-marketing)" and "DNA hack could make medical privacy impossible (https://www.csoonline.com/article/730015/dna-hack-could-make-medical-privacy-impossible)". (Now, we all know that editors will sometimes write sensational headlines in order to draw in readers, but I have to just say "*Please, Editors... Take a deep breath and maybe a Xanax*".)

The more complicated reality is that, while this recent re-identification demonstration provided some important warning signals for future potential health privacy concerns, it was not likely to have been implemented by anyone other than an academic re-identification scientist; nor would it have been nearly so successful if it had not carefully selected targets who were particularly susceptible for re-identification.

As I've written elsewhere, from a public policy standpoint, it is essential that the re-identification scientists and the media accurately communicate re-identification risk research (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397); because public opinion should, and does, play an important role in setting priorities for policy-makers. There is no "free lunch". Considerable costs come with incorrectly evaluating the true risks of re-identification, because de-identification practice importantly impacts the scientific accuracy and quality of the healthcare decisions made based on research using de-identified data. Properly balancing disclosure risks and statistical accuracy is crucial because some popular de-identification methods can unnecessarily, and often undetectably, degrade the accuracy of de-identified data for multivariate statistical analyses. Poorly conducted de-identification may fail to protect privacy, and the overuse of de-identification methods in cases where they do not produce meaningful privacy protections can quickly lead to undetected and life threatening distortions in research and produce damaging health policy decisions.

So, what is the realistic magnitude of re-identification risk posed by the "Y-STR" surname inference re-identification attack methods developed by Yaniv Erlich's (https://blogs.law.harvard.edu/billofhealth/2013/05/23/breaking-good-a-short-ethical-manifesto-for-the-privacy-researcher/) lab? Should *everyone* really be fearful that this "DNA Hack" has now made their "medical privacy impossible"?The Science article (https://www.sciencemag.org/content/339/6117/321.abstract) and supplementary materials (https://www.sciencemag.org/content/suppl/2013/01/16/339.6117.321.DC1/1229566.Gymrek.SM.pdf) describing these methods provide some necessary details for properly contextualizing this risk. Of course, only genomic specimens from males are directly at risk for this attack, which makes use of the relationship between Short Tandem Repeats (STRs) on the Y chromosome and culture norms for paternally inherited surnames; so, 50 percent of the population (i.e., females) are not at direct risk of re-identification from this attack. Furthermore, the analyses indicated that even when the surname prediction method was tuned to its optimal confidence threshold, no surname could be predicted for 83 percent of the males on which it was tested and that incorrect (false positive) surnames would be predicted for another 5 percent of the males. Thus, according to Erlich's own published estimates, only about 6 percent of the U.S. population is at risk of having their last name correctly guessed from this method; and 94 percent of the population was not at risk of even having the method provide a correct guess at their last name. For real-world uses (like attempts to use the method for life insurance discrimination), this quite low surname recovery rate importantly limits the economic viability of attempting such attacks. But such attacks would also face even further dramatic reductions in their successful implementation.

Under the Hood

As we continue our critical look under the hood of this re-identification attack, it should be clear that just having a method that provides a guess (which is quite possibly incorrect) at someone's last name isn't equivalent to re-identifying them. Once a surname has been guessed there may be thousands, perhaps many thousands, of men in the U.S. who also share this guessed last name. So additional demographics such as an individual's state of residence and age in years (both permissible in HIPAA de-identified data) could possibly be used (if also available with the genomic data) in an attempt to uniquely identify the males associated with genomic samples. Erlich's lab undertook extensive simulations with U.S. Census data and their results (shown in Figure 1D of their paper) estimate that about 17-18 percent of males in the U.S. might be unique with regard to the combination of surname, age in years and state of residence. So of the 12 in 100 U.S. males who could be at risk of re-identification if they had genomic samples available for attack along with their age in years and state of residence, Erlich's simulation results indicate that it would be likely that only 2 or 3 (<20 percent) of them would be unique and therefore potentially re-identifiable.

However, in a real-world implementation of such an attack, the data intruder (a re-identification trade-jargon term for someone who is out to undertake this sort of re-identification malfeasance), having made use of the guessed last name for a target individual and then searched (using age and state) to find any unique individuals, would not know whether the last name supplied by the method was correct (a True Positive (TP)) or incorrect (a False Positive (FP)). Erlich's results, however, indicate that the probability that the guessed last name was actually correct would only be around 70 percent (=TP/(TP+FP) or 0.12/(0.12+0.05)). This is important because it creates a final even more serious impediment to practical use of the method to attempt to re-identify and discriminate against individuals on the basis of their genomic data.

Consider the results that would occur if in the future some misguided life insurance company decided to implement such an attack on 100,000 males in an attempt to decline unprofitable policies (assuming that genomic information was routinely available, still not provided the legal protections that this demonstration attack begs for, and that in the future such sufficiently accurate determination of the relationship between genomic risks and all causes of death would become feasible). Of the 100,000 males, the insurance company would be able to obtain a last name guess for 17,000 of them (=100,000 x 17 percent prediction – whether correct or incorrect- rate). Of these 17,000, only about 3,000 (= 17,000 x 17-18 percent unique) would likely be unique with regard to their age and state. But of these 3,000, almost 900 of them (= 3,000 x 30 percent FP rate) would have had incorrect predictions regarding their last names. If the insurance company, having incurred the expense of implementing the method on 100,000 men, wished to decline policies for these 3,000 men, they would also need to throw away 900 (nearly one third) profitable customers for no good reason. The simple economics of the probabilities underlying this attack method seem to make its potential use questionable, even if we suppose that society learned nothing from the vulnerabilities that have been exposed by this re-identification attack and did not act to appropriately provide necessary protections.

So how did this re-identification attack with rather limited potential succeed in grabbing and holding the degree of media attention and sensation that it did? By steering away from the risks facing the general population and instead picking a particularly susceptible population where the chance of success and associated effort involved in providing proof-of-concept for these attacks would be feasible and sufficiently remarkable to hold the public's attention.

"Soft Targets"

Attempts to demonstrate proof-of-concept on three identified genomes resulted in re-identification for one of the targets (Craig Venter); but, to demonstrate that this was not a fluke, journal reviewers wanted proof (https://www.nature.com/news/privacy-protections-the-genome-hacker-1.12940) that completely anonymous donors could be identified. So the authors turned to an already well documented "soft target", "CEU" participants who had originally had their samples collected by CEPH (Centre d'Etude du Polymorphisme Humain) consisting of multigenerational families of Northern and Western European ancestry in Utah which had been later re-consented to participate in the HapMap project. A paper by Gitschier had already exposed the vulnerabilities of CEU participants (https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2668019/pdf/main.pdf) through Y-STR attack methods almost four years earlier and had confirmed that potential surnames could be detected among the CEU participants. (I'll have more to say later contrasting the Gitschier study with that of the Erlich lab). Additionally, the CEU targets had the advantage that the informed consent of these individuals did not definitively guarantee their privacy and stated that future techniques might be able to identify them.

Erlich's lab selected the 10 CEU participant genomes that had the most complete Y-STR haplotypes on which to attempt surname recovery. Searching the genetic genealogy databases returned top-matching records with Mormon ancestry in 8 of the 10 individuals. The dramatic re-identification advantage that this provided is actually clearly spelled out by the authors indicating that the high surname recovery rate

> stems from a combination of the deep interest in genetic genealogy among this population and the large family sizes, which **exponentially** increases the number of targeted individuals for every person who is tested. *[Emphasis added]*

Because of this, it is not particularly surprising that, within this usually vulnerable set of CEU test cases, from five initial CEU surname recovery cases, Erlich's lab was able to identify three pedigrees (and in two of these pedigrees infer both the surnames of paternal and maternal grandfathers) and thus breach the privacy of nearly 50 individuals through this pedigree amplification step. However, the success of this surname inference attack method clearly would not have been nearly so remarkable if Erlich had instead sought to document the impact of the attacks on a random sample of the U.S. male population. So in spite of this final diversionary step, the reality remains that what made the headlines for this research was not the realistic risks facing most of the U.S. public, but rather a proof-of-concept targeting an exceptionally vulnerable sub-population.

Necessary Proof

Please don't read me wrong about the value of this proof-of-principle. The risks associated with this attack are likely to only increase over the next decade or so. Now is clearly the time for sage public policy-makers to be thinking deeply about the re-identification risks associated with genomic data and designing appropriate protections (https://www.ncbi.nlm.nih.gov/pubmed/23449577) which "*augment imperfect technical safeguards with measures that make such re-identification socially, legally, and economically unacceptable*", not only for this attack, but for others that are sure to be devised in the future. Given the inherent extremely large combinatorics of genomic data and the intrinsic biological and social network characteristics that determine how genomic traits (and, as we've been reminded, surnames) are shared with both our ancestors and descendants through genealogic lines, issues surrounding the degree to which such information can be meaningfully "de-identified" (https://blogs.law.harvard.edu/billofhealth/2013/05/22/re-identification-is-not-the-problem-the-delusion-of-de-identification-is-re-identification-symposium/) are non-trivial. I'll say more about this point, especially vis-à-vis the HIPAA de-identification standards, later in the symposium.

Call for Action: Legislation Prohibiting Re-identification

At present, elimination or further reduction of both the age and location information associated with the genomic information could have thwarted the surname inference attack; but even more importantly, this demonstration attack cries out for legislative action to impose civil and criminal penalties for re-identification attempts. Carefully crafted legislation prohibiting re-identification attempts could still allow Institutional Review Board (IRB) approved re-identification research to be conducted but would ban any re-identification attempts conducted without essential human subjects research protections. I've provided further public policy recommendations for better controlling re-identification risks (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2076397), and I'll be writing more about this topic in Part 2 of this essay.

"So Easy, Anyone Can Do It"

A consistent theme in the inquiry-deficient and often downright lazy media coverage on this attack was how "easy" it was to do, supposedly requiring no more than an internet connection and some free time. However, a quick skim of the four-page paper in Science and the 39 pages of supplementary materials will convince anyone who isn't a PhD-level geneticist/computational biologist that attack was fiendishly clever and anything but easy. Still, as much as Erlich's lab might now be able to publish a "*Do-it-yourself Guide to Identifying Personal Genomes by Surname Inference*" for the final internet search steps in this elaborate attack, it should be quite clear that conducting this attack from inception to conclusion required a genetics lab with all of the necessary laboratory, computational and financial resources, along with a large team with the brain-power and pre-requisite decades of academic training that the Erlich

Lab (https://erlichlab.wi.mit.edu/) and the Whitehead Institute (https://wi.mit.edu/people/fellows/erlich) could provide. Because there are great benefits created by research on de-identified data (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1789749) and health-related harms would result from abandonment of de-identification, which clearly provides effective deterrence and privacy protections relative to having direct identifiers present, the cost-benefit calculus for de-identification public policy is complex and could benefit greatly from a detailed accounting of the resources and expense involved in setting up the Erlich Lab and running the attacks from inception to conclusion. Based on the calculations that I presented above for success in the general U.S. male population, my guess is that having an accurate handle on the total costs per achieved re-identification would be useful information for policy-makers grappling with the near and long-term ramifications of this attack.

In this regard, I think the Erlich attack serves as an outstanding example of what I believe is an inherently distortive influence that re-identification demonstrations have typically had (https://www.concurringopinions.com/archives/2012/09/re-identification-risks-and-myths-superusers-and-super-stories-part-i-risks-and-myths.html) on the development of sound, prudent and logical public policy (https://www.concurringopinions.com/archives/2012/09/re-identification-risks-and-myths-superusers-and-super-stories-part-ii-superusers-and-super-stories.html). Many, if not most, re-identification demonstration attacks, particularly because of the way their results have been reported to the public, serve to inherently distort the public's (and, perhaps, policy-makers'?) perceptions of the likelihood of "real-world" re-identification risks. However, most demonstration attacks are typically conducted by highly skilled scientists assisted by very bright but inexpensive graduate student labor. Such attackers draw on academic sources of financial support and thus can afford the considerable computational and data resources and requisite time and efforts to achieve re-identifications that would often have little actual economic incentive in the everyday life, at least when they are directed at data which has been reliably de-identified under the HIPAA Expert Determination De-identification Method (https://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html) which requires that:

> A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable: applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information.

Although unanticipated attack methods will continue to arise occasionally, the fundamentals underlying re-identification risks are actually fairly straightforward to anticipate in advance: Combinations of high resolution information (e.g. full dates of birth and 5-digit Zip Codes) which are matters of public record or otherwise so widely available such that it becomes possible to economically and reliably build a near perfect population register should be anticipated to pose important potential re-identification risks. This still doesn't mean that real -life re-identifications will be likely, due to the time, effort and expense involved in building such population registers and the fact that most people likely don't have any motivation to undertake such attacks, but at least it isn't complicated to realize when such attacks might be feasible. I'll also say more on this point in Part 2 of this essay.

Re-identification Researcher/Media Common Interests?

Do combined re-identification researcher and media motivations create important potential conflicts of interest for reporting of re-identification attacks? Arvind Narayanan has posed some provocative questions in his symposium contribution (https://blogs.law.harvard.edu/billofhealth/2013/05/26/reidentification-as-basic-science/):

> What really drives reidentification researchers? Do we publish these demonstrations to alert individuals to privacy risks? To shame companies? For personal glory? If our goal is to improve privacy, are we doing it in the best way possible?

Unfortunately, I think if we are honest here, there may be incentives for re-identification scientists and the media to join forces (unintentionally or not) in overstating real-life re-identification risks in attempts by editors and writers to drum up a media audience or by researchers seeking to promote their research and, thus, their promotion and tenure.

However, given that over-application of de-identification comes at very tangible costs to statistical accuracy of research conducted with de-identified data (because unnecessary de-identification will mask important heterogeneities between subgroups or destroy the integrity of variance-covariance matrices for multivariate statistical methods), we should be concerned that even broader and troubling social harms will likely result from the over-sensationalizing of re-identification risks.

Fueled by Fear

Unfortunately, humans (whether they are the general public, politicians or policy-makers) have a demonstrated diminished capacity to rationally assess and respond to probabilities and risks when fear is invoked (https://papers.ssrn.com/sol3/papers.cfm?abstract_id=967372). But fear sells newspapers, and addressing a subject which we should truly fear means our research has great importance and relevance. Thus, when a re-identification attack has been brought to life, like some Frankenstein monster, our assessment of the probability of it actually being implemented in the real-world may subconsciously become 100 percent, which is highly distortive of the true risk/benefit calculus that we face.

Realistic Risk Assessments

Real-world risks usually face very pragmatic economic disincentives when someone who needs to make a profit re-identifying people (at least when the data has been properly de-identified with these data intrusion motivations and considerations properly taken into account (https://www.cbs.nl/NR/rdonlyres/C3E1B07E-1893-4809-9955-50DEA2B9ADA6/0/nos991.pdf), as was wisely advocated by disclosure risk researchers Elliot and Dale more than a decade ago). As Elliot and Dale note, when proper de-identification methods have been used to effectively reduce re-identification risks to very small levels, it becomes highly unlikely that data intruders would conclude that it is worth the time, effort and expense to undertake a re-identification attempt in the first place. With use of proper de-identification best practices, midnight dumpster diving to look for prescription bottles is likely to become the more economically viable approach to violating our neighbors' privacy (if we are inclined toward this type of malfeasance).

There are often many unknowns in evaluation of such re-identification scenarios. In cases where it is not readily apparent that the re-identification risks must be very small on the basis of highly unlikely preconditions for the attack, policy-makers should pursue the use of quantitative policy analyses using state-of-the-art uncertainty and sensitivity analysis methods (https://books.google.com/books/about/Uncertainty.html?id=ajd1V305PgQC). These methods have been routinely utilized by agencies such as the Department of Energy or the Environmental Protection Agency for decades for policy evaluations when substantial uncertainty exists regarding the parameters that underlie such risk assessments.

Surely if we rely on such complex quantitative policy analysis methods to produce risk assessments in arenas of potentially catastrophic harm where we face important uncertainties (like nuclear safety or climate change), these very same methods could and should be used to help provide robust policy guidance in the area of re/de-identification privacy policy. Privacy scientists and policy-makers should pursue such policy analyses in collaborative

efforts conducted with transparency rather than allowing our debates to be steered astray when privacy alarmists wield anecdotes of rare re-identifications — most of which have been achieved through demonstration attacks conducted by academic privacy researchers and only after great effort and too often without important verification of the purported re-identifications (https://www.plosone.org/article/info%3Adoi%2F10.1371%2Fjournal.pone.0028071).

Final Questions

Having raised what I believe are important considerations about how much this re-identification attack (and, unfortunately, other attacks both before and after this demonstration) reflects the true risks from such attacks, and the combined role that re-identification researcher and the media have in communicating these risks, I have some final questions to add to the list of excellent questions posed by Arvind:

- Is it an ethically compromised position, in the coming age of personalized medicine, if we end up purposefully masking the racial, ethnic or other group membership status information (e.g. American Indians or LDS Church members, etc.) for certain individuals, or for those with certain rare genetic diseases/disorders, in order to protect them against supposed re-identification, and thus also deny them the benefits of research conducted with de-identified data that may help address their health disparities, find cures for their rare diseases, or facilitate "orphan drug" research that would otherwise not be economically viable, especially if those re-identification attempts may not be forthcoming in the real-world (demonstration attacks by scientists not withstanding)?
- Are re-identification researchers doing all that they can to publically correct any inaccurate press with regard to the results and implications of their work?

In my next post, I'll address the recent Personal Genome Project (PGP) re-identification attack. I'll also discuss some of the cultural norms/ethos of both the *statistical disclosure control* and the *computer security/privacy* research communities and try to shed some light on the background assumptions each of these groups bring to the table, and how this "culture clash" can impact our perspectives on ethical conduct of re-identification research.

2 thoughts to "Public Policy Considerations for Recent Re-Identification Demonstration Attacks on Genomic Data Sets: Part 1 (Re-Identification Symposium)"

SHERRY @CASCADIA

June 14, 2013 at 11:32 pm (https://blog.petrieflom.law.harvard.edu/2013/05/29/public-policy-considerations-for-recent-re-identification-demonstration-attacks-on-genomic-data-sets-part-1-re-identification-symposium/#comment-621)

Some of us who grew up in the AIDS community have a more nuanced concern about the ability to identify patients from a larger pool at the individuale level that has little to do with the identification questions.

1) When a provider is given a quality score will they identify those patients that "bring their score down" and drop them from their panel "as being non-compliant?' (we are already seeing this happen)

2) Will your diagnosis or problem list result in drug companies targeting your provider to prescribe a new drug vs a generic? (yes one of the "free" EHR's is in fact based on this business model).

3) In the case of parents or patients who have different values and or preferences IE will patients like those in a recent Kaiser study who opted for diet and exercise before a Staten or Parents who's preferences or values result in them choosing a different vaccination schedule be labeled non-compliant in their "permanent health record?

4) Although health care providers have no privacy protections will the open exchange of patient data also expose women's health care providers (those that provide pregnancy termination services) to additional risk from those that oppose the procedure? (ie every nurse and doctor who provides the services are now searchable and we know this can be a life threatening situation for the docs and other staff – yes I realize it would be unethical to mine the data that way but it only takes one or two radicals to find the information)

None of these examples are meant to stop the free and open exchange of health data it just raises the secondary impact that we need to be aware of and mitigate.

Log in to Reply (https://blog.petrieflom.law.harvard.edu/wp-login.php?redirect_to=https%3A%2F%2Fblog.petrieflom.law.harvard.edu%2F2013%2F05%2F29%2Fpublic-policy-considerations-for-recent-re-identification-demonstration-attacks-on-genomic-data-sets-part-1-re-identification-symposium%2F)

DANIEL BARTH-JONES

June 15, 2013 at 1:33 pm (https://blog.petrieflom.law.harvard.edu/2013/05/29/public-policy-considerations-for-recent-re-identification-demonstration-attacks-on-genomic-data-sets-part-1-re-identification-symposium/#comment-623)

If I'm understanding your comments correctly, Sherry, the issues that you are raising are not so much directly related to those of re-identification, but rather data-based decisions which raise issues about the analysis of patient data and application of predictive data models in ways that can impact patient care (or even the care providers) when the individuals are identified or, in some cases, even when they are not.

It is useful to call attention to such concerns, but, as a public policy issue, this highlights a particularly challenging tension: The foundations supporting medical and public heath science and the improvement of our healthcare practices and systems are all based on exactly the same sort of data analysis — and data analysis can be used in ways that are beneficial (thankfully, this by far the predominate case), but, sometimes, might also cause harms.

I agree with your position that none of these examples would be best addressed by stopping free and open exchange of health data and also agree that it is important to be aware of the secondary impacts that can results from our analyses, so negative impacts of such analyses can be appropriately mitigated.

Log in to Reply (https://blog.petrieflom.law.harvard.edu/wp-login.php?redirect_to=https%3A%2F%2Fblog.petrieflom.law.harvard.edu%2F2013%2F05%2F29%2Fpublic-policy-considerations-for-recent-re-identification-demonstration-attacks-on-genomic-data-sets-part-1-re-identification-symposium%2F)

LEAVE A REPLY

You must be logged in (https://blog.petrieflom.law.harvard.edu/wp-login.php?redirect_to=https%3A%2F%2Fblog.petrieflom.law.harvard.edu%2F2013%2F05%2F29%2Fpublic-policy-considerations-for-recent-re-identification-demonstration-attacks-on-genomic-data-sets-part-1-re-identification-symposium%2F) to post a comment.

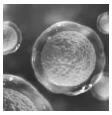
‹ An Open Letter From a Genomic Altruist to a Genomic Extrovert (Re-Identification Symposium) (https://blog.petrieflom.law.harvard.edu/2013/05/29/an-open-letter-from-a-genomic-altruist-to-a-genomic-extrovert-re-identification-symposium/)

Introducing Guest Blogger William MacAskill › (https://blog.petrieflom.law.harvard.edu/2013/05/31/introducing-guest-blogger-william-macaskill/)

Search...

MOST POPULAR

(https://blog.petrieflom.law.harvard.edu/2024/04/04/eu-and-us-regulatory-challenges-facing-ai-health-care-innovator-firms/) EU and US Regulatory Challenges Facing AI Health Care Innovator Firms (https://blog.petrieflom.law.harvard.edu/2024/04/04/eu-and-us-regulatory-challenges-facing-ai-health-care-innovator-firms/)
by The Petrie-Flom Center Staff (https://blog.petrieflom.law.harvard.edu/author/petrieflom/)



(https://blog.petrieflom.law.harvard.edu/2024/04/07/cell-therapies-and-their-legal-discontents/) Cell Therapies and their Legal Discontents (https://blog.petrieflom.law.harvard.edu/2024/04/07/cell-therapies-and-their-legal-discontents/)
by Adithi Iyer (https://blog.petrieflom.law.harvard.edu/author/aiyer/)

(https://blog.petrieflom.law.harvard.edu/2024/04/08/salus-populi-training-the-judiciary-in-the-social-drivers-of-health/) Salus Populi: Training the Judiciary in the Social Drivers of Health (https://blog.petrieflom.law.harvard.edu/2024/04/08/salus-populi-training-the-judiciary-in-the-social-drivers-of-health/)
by The Petrie-Flom Center Staff (https://blog.petrieflom.law.harvard.edu/author/petrieflom/)

(https://blog.petrieflom.law.harvard.edu/2024/04/18/two-years-on-from-a-landmark-abortion-decision-in-kenya/) Two Years On From A “Landmark” Abortion Decision in Kenya (https://blog.petrieflom.law.harvard.edu/2024/04/18/two-years-on-from-a-landmark-abortion-decision-in-kenya/)
by Joelle Boxer (https://blog.petrieflom.law.harvard.edu/author/jboxer/)

(https://blog.petrieflom.law.harvard.edu/2024/04/06/protecting-health-privacy-is-a-royal-pain/) Protecting Health Privacy is a Royal Pain (https://blog.petrieflom.law.harvard.edu/2024/04/06/protecting-health-privacy-is-a-royal-pain/)
by Bobby Stroup (https://blog.petrieflom.law.harvard.edu/author/rstroup/)

GET OUR NEWSLETTER

SUBSCRIBE NOW (HTTPS://PETRIEFLOM.WPENGINE.COM/SIGN-UP-FOR-THE-PETRIE-FLOM-CENTER-NEWSLETTER/)

HOT TOPICS

Select Category

ARCHIVES

Select Month

POWERED BY

The Petrie-Flom Center for Health Law Policy, Biotechnology, and Bioethics at Harvard Law School (https://petrieflom.law.harvard.edu/)

PAGES

About Bill of Health (https://blog.petrieflom.law.harvard.edu/about/)

Policies (https://blog.petrieflom.law.harvard.edu/policies/)

Symposia (https://blog.petrieflom.law.harvard.edu/symposia/)

In Focus Series (https://blog.petrieflom.law.harvard.edu/in-focus/)

SIGN UP FOR OUR NEWSLETTER

SUBSCRIBE (HTTPS://PETRIEFLOM.WPENGINE.COM/SIGN-UP-FOR-THE-PETRIE-FLOM-CENTER-NEWSLETTER/)

FOLLOW US

(https://twitter.com/PetrieFlom)

(https://www.facebook.com/petrieflom/)

(https://vimeo.com/petrieflom)

(https://www.linkedin.com/company/the-petrie-flom/)
