Harmonization Horizon – HIPAA, CCPA, and Other Potential U.S. State Privacy Laws – New Burdens on Medical Research and De-Identified Data?

Ann Waldo, Waldo Law Offices
Daniel Barth-Jones, Columbia University,

March 4, 2020

HIPAA Summit
Arlington, VA

Challenges with CCPA re: health data

Two big problems with CCPA and health data

1) Exemptions for health data are too narrow –
   - Clinical trial data is exempted – but should be clinical research data
   - No exemption for adverse event and device tracking data
2) CA's "deidentification" differs from HIPAA de-identification
   - While simultaneous compliance with both HIPAA and CA de-ID'n standards definitely ***is*** possible….
   - It's also possible for data sets to be de-ID'd per HIPAA but not CCPA
   - Business friction, contracting issues
   - Documentation and compliance costs
   - Terrible precedent for other state and federal law

CCPA def. of “deidentified”

Current CCPA:

“Deidentified” means information that *cannot reasonably identify*, relate to, describe, be capable of being associated with, or be linked, directly or indirectly, to a particular consumer, provided that a business that uses deidentified information:

1) Has implemented technical safeguards that prohibit reidentification of the consumer to whom the information may pertain.
2) Has implemented business processes that specifically prohibit reidentification of the information.
3) Has implemented business processes to prevent inadvertent release of deidentified information.
4) *Makes no attempt to reidentify* the information.

Note differences from HIPAA – ambiguities, focus on business processes

CA Civ Code 1798.140(h)

The 2019 proposed amendments

A set of medical research and healthcare amendments

- To have CCPA recognize HIPAA de-ID'n standard for health data
- To expand clinical research data exemption
- To slightly broaden exemption for HIPAA business associates
- To exempt adverse event and device tracking data

- Broad HC support; agreement reached with privacy advocates
- Amendments weren't enacted, but door opened for 2020

AB 713

- Jan 6 - Sen. Mullin put health amendments into AB 713
- Jan 8 - AB 713 heard in Sen. Health Committee
  - Testifying witnesses were ACRO and AdvaMed
  - Other supporters included United Health Group, CA Hosp Assn, AHIP, BIO, BioCom, CA Life Sciences Assn, IPMPC, Medical Imaging and Technology Alliance, PhRMA, and Waldo Law
  - Privacy coalition expressed neutrality and said they'd been closely collaborating with industry
  - Reported out unanimously by Sen Health Committee

AB 713 – What's Next?

- Post-Sen Health, clarifying amendments written and circulating
- "Urgency clause" added to make it effective immediately
- **The path forward**
  - **Achieve final consensus on details of amendments**
  - **Sen Judiciary, Appropriations report, Senate floor and Assembly concurrence with 2/3 votes, Governor signature**

What about CCPA 2.0/Ballot Initiative?

CA Privacy Rights and Enforcement Act of 2020

- **Yet another definition of de-ID'n with no recognition of HIPAA**

(k) "Deidentified" means information that cannot reasonably be used to infer information about, or otherwise be linked to, an identifiable consumer, provided that the business that possesses the information:
(A) takes reasonable measures to ensure that the information cannot be associated with a consumer or household;
(B) publicly commits to maintain and use the information in deidentified form and not to attempt to reidentify the information, except as necessary to ensure compliance with this subdivision; and
(C) contractually obligates any recipients of the information to comply with al provisions of this subdivision.

Pending Legislation - WA State

- SB 6821 and HB 2742 companion bills
- Enactment in 2020 has been thought likely
- Based on GDPR, not CCPA
- Senate bill has good exemptions for health data and HIPAA de-ID'd data
- House bill lacks these
- Wrangling over private right of action and facial recognition – bills might fail entirely

  - *Even so, including solid health/de-ID'n language would be an excellent precedent for other states, WA in 2021, and federal bills*

Pending Legislation - NY

NY S 5642

- Divergent definition of de-identification. No HIPAA recognition
- Private right of action. Fiduciary duties for data holders

"De-identified data" means:
(a) data that cannot be linked to a known natural person without additional information not available to the controller; or
(b) data (i) that has been modified to a degree that the risk of re-identification is small as determined by a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for de-identifying data, (ii) that is subject to a public commitment by the controller not to attempt to re-identify the data, and (iii) to which one or more enforceable controls to prevent re-identification has been applied. Enforceable controls to prevent re-identification may include legal, administrative, technical, or contractual controls.

Pending Legislation - VA

VA HB 473

- Extremely narrow research exemption
- No HIPAA de-ID'n recognition

"Deidentified data" means:

1. Data that cannot be linked to a known natural person without additional information kept separately; or
2. Data (i) that has been modified to a degree that the risk of reidentification is small, (ii) that is subject to a public commitment by the controller not to attempt to reidentify the data, and (iii) to which one or more enforceable controls to prevent reidentification has been applied. Enforceable controls to prevent reidentification may include legal, administrative, technical, or contractual controls

Consequences of Divergent State Laws

- Already now have divergent HIPAA and CCPA de-ID'n standards – should document how de-ID'd data meets both definitions
- *How to manage if more than two de-ID'n standards?*
- Narrowness of research and BA exemptions; inclusion of adverse event and tracking data in consumer laws
  - Compliance and operational costs
  - Uncertainty
  - Contractual wrangling; legal disputes and costs
  - Business friction and delays
  - Some data projects may just not be possible under state law
  - Mounting cost of new drugs and devices

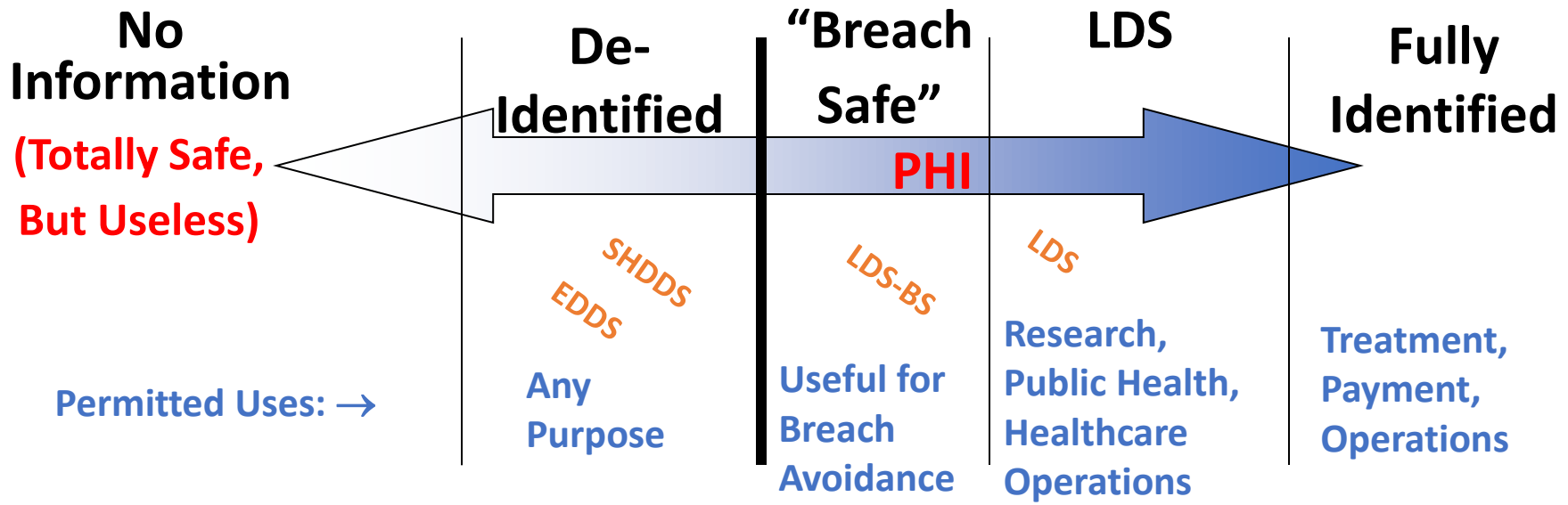
What can be done to show support for medical research and de-ID'd data?

State recognition of federal standards for medical research, HIPAA, Common Rule, and de-ID'n of health data is imperative

Good state legislation and definitions will create solid precedents for federal legislation

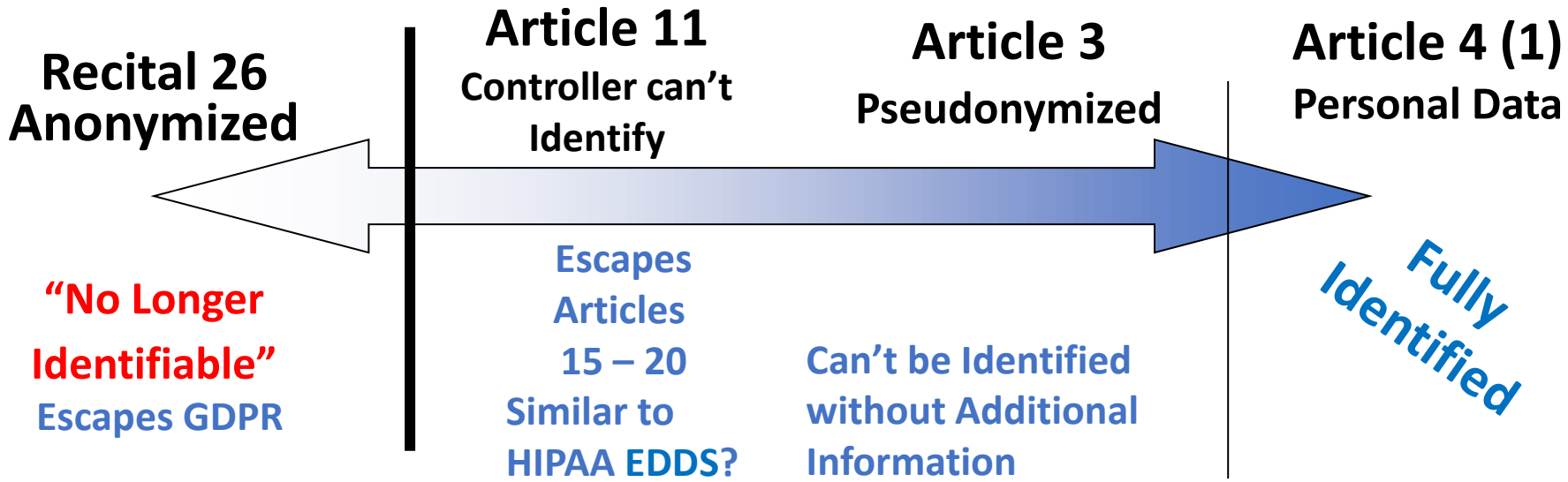
- ***Support medical research by advocating for consistent HIPAA de-ID'n standard nationwide***
- ***Oppose inconsistent de-ID'n standards that will lead to friction, legal cost, waste – and research delays***

HIPAA's Identification Spectrum

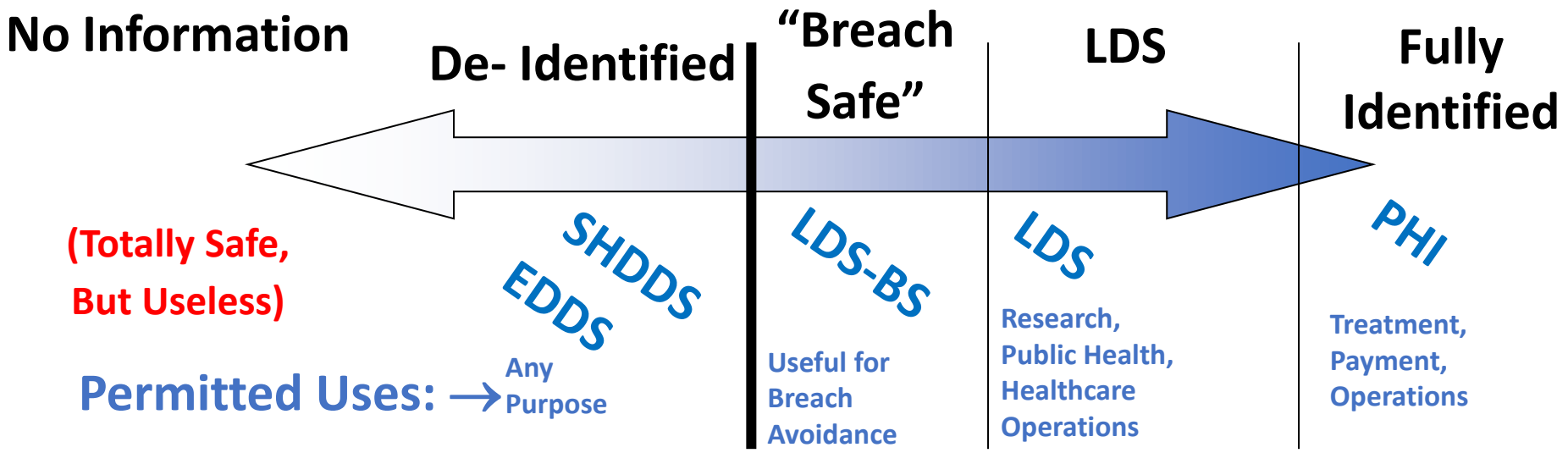


- **Protected Health Information (PHI)**
- **Limited Data Set** (LDS) §164.514(e)
  - Eliminate 16 Direct Identifiers (Name, Address, SSN, etc.)
- **LDS w/o 5-digit Zip & Date of Birth** (LDS-"Breach Safe") 8/24/09 FedReg
  - Eliminate 16 Direct Identifiers ***and Zip5, DoB***
- **Safe Harbor De-identified Data Set (SHDDS)** §164.514(b)(2)
  - Eliminate 18 Identifiers (including Geo < 3 digit Zip, All Dates except Yr)
- **Expert Determination Data Set (EDDS)** §164.514(b)(1)
  - Verified "very small" Risk of Re-identification

GDPR's Identification Spectrum



HIPAA's Identification Spectrum



The New York State Senate

Senate Bill S5642

2019-2020 Legislative Session

NON-PUBLIC COMMUNICATIONS, AND INFORMATION REGARDING AN INDIVIDUAL'S INTERACTION WITH AN INTERNET WEBSITE, MOBILE APPLICATION, OR ADVERTISEMENT;

(VI) HISTORICAL OR REAL-TIME GEOLOCATION DATA;

(VII) AUDIO, ELECTRONIC, VISUAL, THERMAL, OLFACTORY, OR SIMILAR INFORMATION;

(VIII) EDUCATION RECORDS, AS DEFINED IN SECTION THIRTY-THREE HUNDRED TWO OF THE EDUCATION LAW;

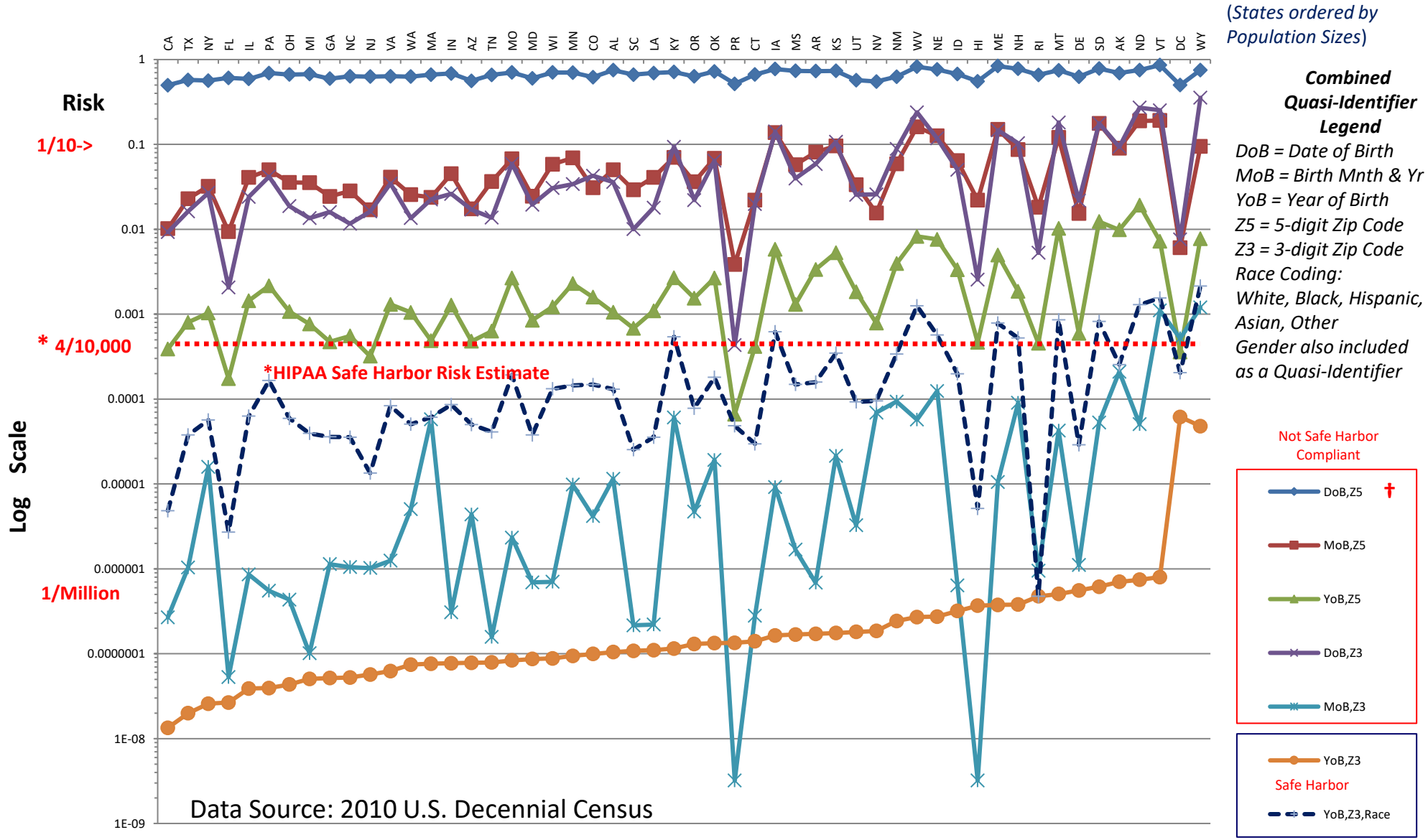
(IX) POLITICAL INFORMATION OR INFORMATION ON CRIMINAL CONVICTIONS OR ARRESTS;

(X) ANY REQUIRED SECURITY CODE, ACCESS CODE, PASSWORD, OR USERNAME NECESSARY TO PERMIT ACCESS TO THE ACCOUNT OF AN INDIVIDUAL;

(XI) CHARACTERISTICS OF PROTECTED CLASSES UNDER THE HUMAN RIGHTS LAW, INCLUDING RACE, COLOR, NATIONAL ORIGIN, RELIGION, SEX, AGE, OR DISABILITY; OR

(XII) AN INFERENCE DRAWN FROM ANY OF THE INFORMATION DESCRIBED IN THIS PARAGRAPH TO CREATE A PROFILE ABOUT AN INDIVIDUAL REFLECTING THE INDIVIDUAL'S PREFERENCES, CHARACTERISTICS, PSYCHOLOGICAL TRENDS, PREFERENCES, PREDISPOSITIONS, BEHAVIOR, ATTITUDES, INTELLIGENCE, ABILITIES, OR APTITUDES. **<-or in other words, "Science"**

U.S. State Specific Re-identification Risks: Population Uniqueness

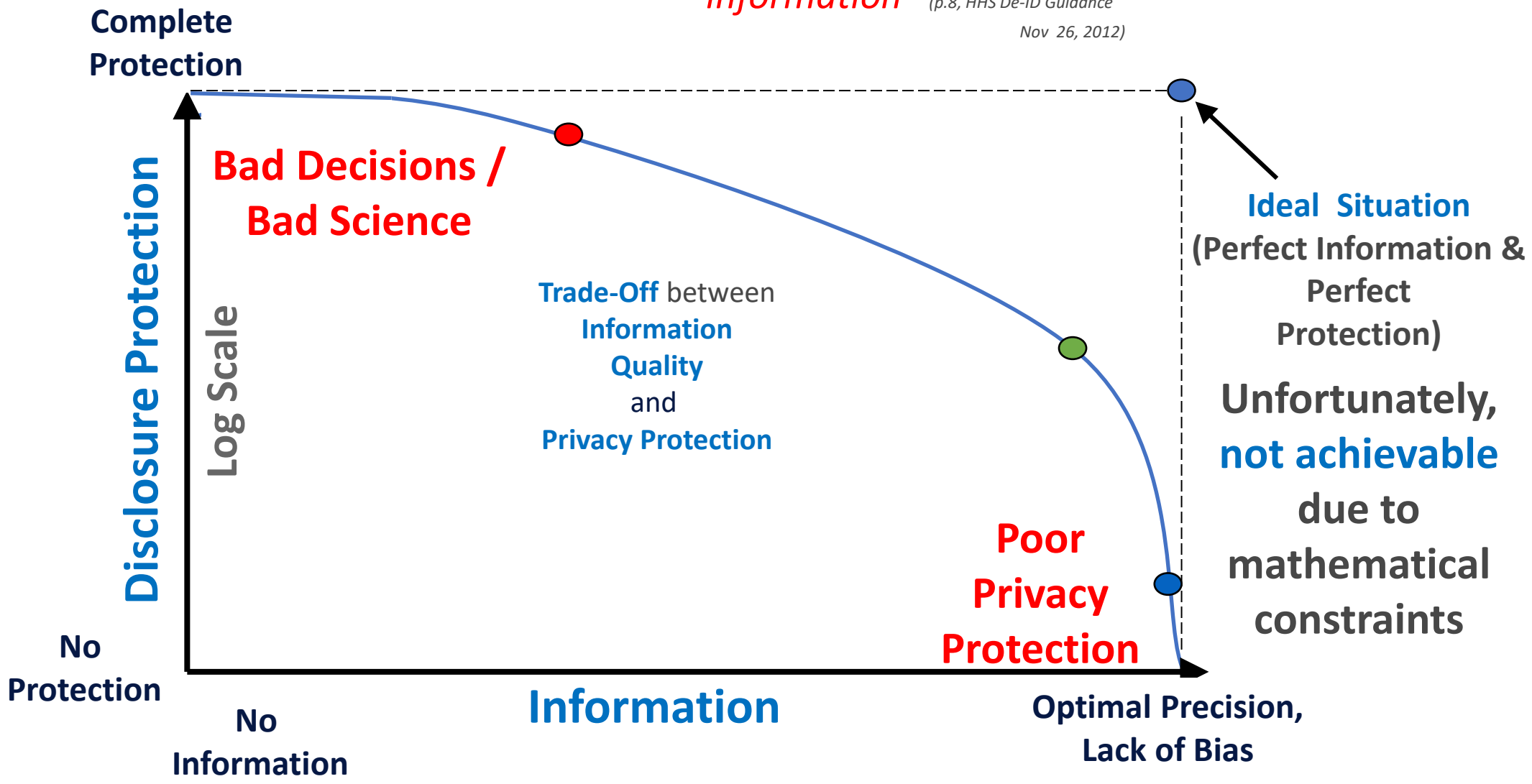


Graph © DB-J 2013

† *HIPAA Safe Harbor does not permit any Dates more specific than the year, or Geographic Units smaller than 3-digit Zip Codes (Z3).*

The Inconvenient Truth:

"De-identification leads to information loss which may limit the usefulness of the resulting health information" *(p.8, HHS De-ID Guidance Nov 26, 2012)*

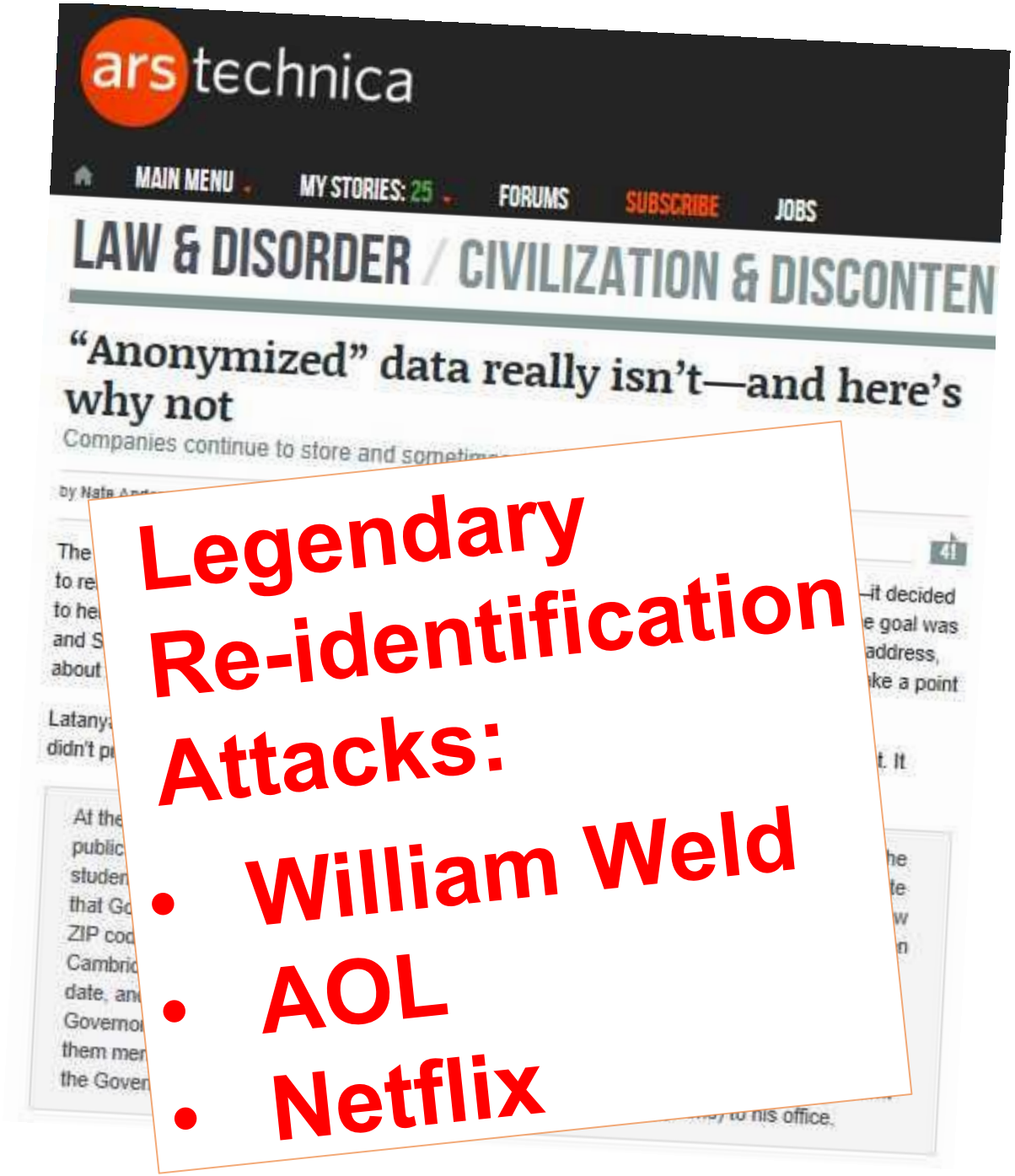


57 UCLA LAW REVIEW 1701 (2010)

BROKEN PROMISES OF PRIVACY: RESPONDING TO THE SURPRISING FAILURE OF ANONYMIZATION

Paul Ohm*

Computer scientists have recently undermined our faith in the privacy-protecting power of anonymization, the name for techniques that protect the privacy of individuals in large databases by deleting information like names and social security numbers. These scientists have demonstrated that they can often "reidentify" or "deanonymize" individuals hidden in anonymized data with astonishing ease. By understanding this research, we realize we have made a mistake, labored beneath a fundamental misunderstanding, which has assured us much less privacy than we have assumed. This mistake pervades nearly every information privacy law, regulation, and debate, yet regulators and legal scholars have paid it scant attention. We must respond to the surprising failure of anonymization, and this Article provides the tools to do so.



Unfortunately, de-identification public policy has often been driven by largely anecdotal and limited evidence, and re-identification demonstration attacks targeted to particularly vulnerable individuals, which fail to provide reliable evidence about real world re-identification risks

Misconceptions about HIPAA De-identified Data:

"It doesn't work…" "easy, cheap, powerful re-identification" (Ohm, 2009 "*Broken Promises of Privacy*")

****Pre-HIPAA*** Re-identification Risks {Zip5, Birth date, Gender} able to identify **87%**?**, 63%, 28%**? of US Population (Sweeney, 2000, Golle, 2006, Sweeney, 2013)

- Reality: HIPAA compliant de-identification provides important privacy protections
  - Safe harbor re-identification risks have been estimated at 0.04% (4 in 10,000) (Sweeney, NCVHS Testimony, 2007)
- Reality: Under HIPAA de-identification requirements, re-identification is expensive and time-consuming to conduct, requires substantive computer/mathematical skills, is rarely successful, and usually uncertain as to whether it has actually succeeded

Misconceptions about HIPAA De-identified Data:

"It works perfectly and permanently…"

- Reality:
  - Perfect de-identification is not possible.
  - De-identifying does not free data from all possible subsequent privacy concerns.
  - Data is never permanently "de-identified"…
    - There is no 100% guarantee that de-identified data will remain de-identified regardless of what you do with it after it is de-identified.

Re-identification Demonstration Attack Summary

Re-identification Attacks	Quasi-Identifers (w/ HIPAA Safe Harbor exclusion data in Red)	Vulnerable Subgroup Targeted?	Table	Individuals w/ Alleged/Verified Re-identification	At-Risk Sample Size	Notable Headlines & Quotes	Attack Against HIPAA Compliant (or SDL Protected) Data?	Demonstrated Re-identification Risk
Governor Weld [1,2]	Zip5, Gender, DoB	Yes	No	n=1	99,500	*"Anonymized" Data Really Isn't* [27]	No	0.00001
AOL [3]	Free Text from Search Queries w/ Name, Location, etc	Yes	No	n=1	657,000	*A Face is Exposed* [3]	No	0.0000015
Netflix [4]	Movie Ratings & Dates	Yes	No	n=2	500,000	*"...successfully identified 99% of people in Netflix database"* [28]	No	0.000004
ONC Safe Harbor [5]	Zip3, YoB, Gender, Marital Status, Hispanic Ethnicity	No	N/A	n=2	15,000	[Press Did Not Cover This Study]	Yes	0.00013
Heritage Health Prize [6,7,8,9]	Age, Sex, Days in Hospital, Physician Specialty, Place of Service, CPT Code, Days Since First Claim, ICD-9 Diagnosis	Yes	No	n=0	113,000	*To best of my judgment, reidentification is within realm of possibility* [8] *El Emam estimated < 1% of Pts could be re-identified. Narayanan estimated > 12% of Pts were identifiable.* [29]	Yes	0.0
Y-Chromosome STR Surname Inference [10,11] - Simulation Study Part	Y-STR DNA Sequences* Age in Years & State	No	N/A, Simulation	Not Attempted: Simulated Results	~150 Million US Males	*"nice example of how simple it is to re-identify de-identified samples"* [30]	*No? (Safe Harbor vs. Expert Determination) *Safe Harbor Excludes: Any unique identifying #, characteristic or code	.12 (For Males Only), after accounting for 30% False Positive Rate
- CEU Attack Part	Age, Utah State, Genealogy Pedigrees & Mormon Ancestry	Yes, Highly Targeted	No	n=5 w/ Y-STR Alone, (but w/ Geneology Amplification n=50)	?	*DNA Hack Could Make Medical Privacy Impossible* [31]		Not Clearly Calculable for CEU Attack
Personal Genome Project [12,13,14]	Zip5, Gender, DoB	No	N/A	n=161	579	*"...re-identified names of > 40% anonymous participants"* [32] *re-identified 84 to 97% of sample of PGP volunteers* [33]	No	0.28 (w/ Embedded Names Excluded)
Washington St. Hospital Discharge [15,16]	Hospital Data w/ Diagnoses, Zip5, Month/Yr of Discharge	Yes	No	n=40 (8 verified) from 81 News Reports	648,384	*"...how new stories about hospital visits in Washington State leads to identifying matching health record 43% of the time"* [34]	No	0.000062
Cell Phone "Unicity" [17]	High Resolution Time (Hours) and Cell Tower Location	No	N/A	Not Attempted	1.5 Million	*"four spatio-temporal points enough to uniquely identify 95%"* [17]	No	0.0
NYC Taxi [18,19]	High Resolution Time (Minutes) and GPS Locations	Yes	No	n=11	173 Million Rides	*How Big Brother Watches You With Metadata* [35]	No	0.0000001
Credit Card "Unicity" [20,21,22,23,24,25,26]	High Resolution Time (Days), Location and Approx. Price	No	N/A	Not Attempted	1.1 Million	*With a Few Bits of Data, Researchers Identify 'Anonymous' People* [36]	No	0.0

- *Publicized attacks are on data without HIPAA/SDL de-identification protection.*
- *Many attacks targeted especially vulnerable subgroups and did not use sampling to assure representative results.*
- *Press reporting often portrays re-identification as broadly achievable, when there isn't any reliable evidence supporting this portrayal.*

Re-identification Demonstration Attack Summary

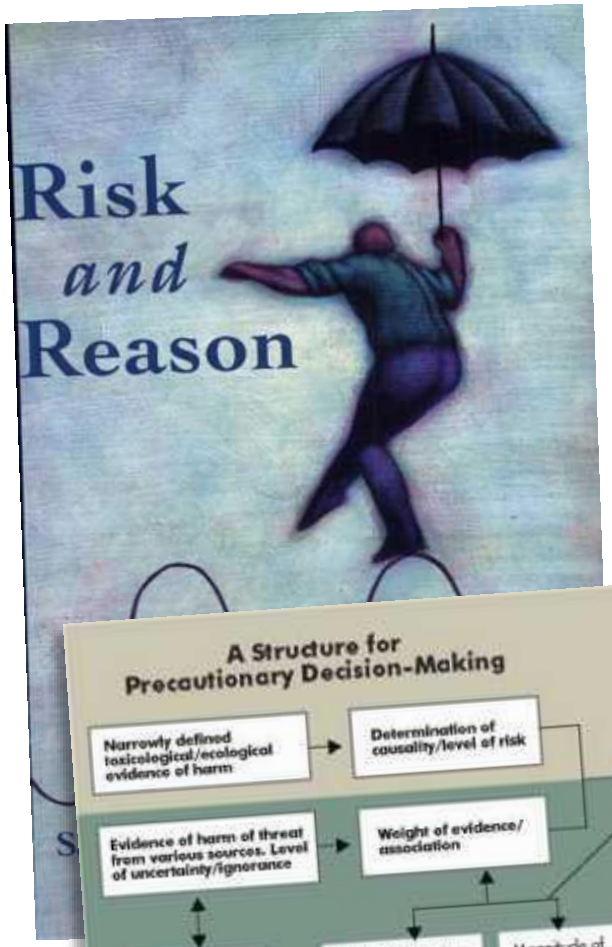
- For Ohm's famous "Broken Promises" attacks (Weld, AOL, Netflix) a total of n=4 people were re-identified out of 1.25 million.
- For attacks against HIPAA de-identified data (ONC, Heritage*), a total of n=2 people were re-identified out of 128 thousand.
  - ONC Attack Quasi-identifers: Zip3, YoB, Gender, Marital Status, Hispanic Ethnicity
  - Heritage Attack Quasi-identifiers*: Age, Sex, Days in Hospital, Physician Specialty, Place of Service, CPT Procedure Codes, Days Since First Claim, ICD-9 Diagnoses (*not complete list of data available for adversary attack)
  - Both were "adversarial" attacks.
- For all attacks listed, a total of n=268 were re-identified out of 327 million opportunities.

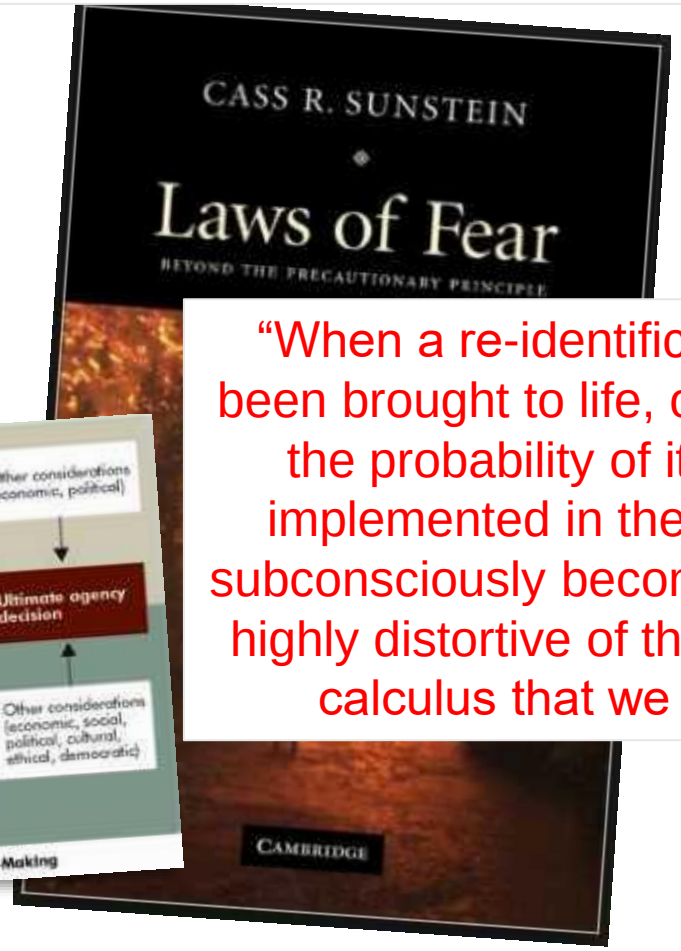
Let's get some perspective on this…

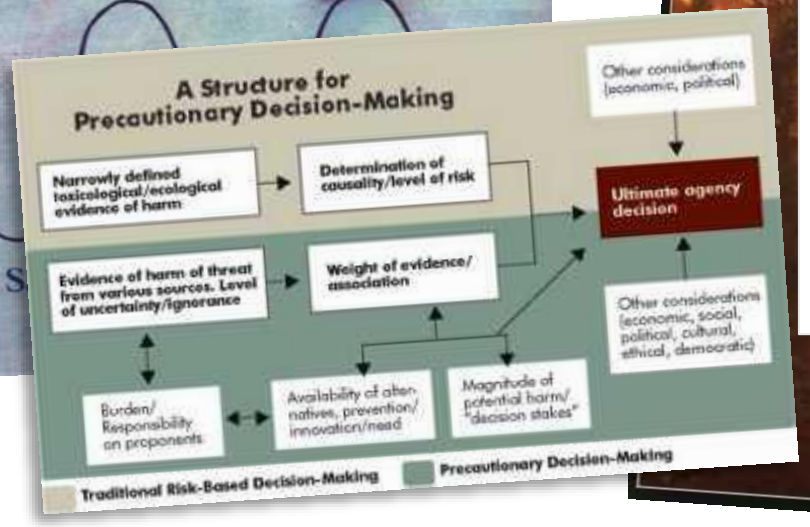
Obviously, This slide is **BLACK**

So clearly, De-identification Doesn’t Work.

Precautionary Principle or Paralyzing Principle?







"When a re-identification attack has been brought to life, our assessment of the probability of it actually being implemented in the real-world may subconsciously become 100%, which is highly distortive of the true risk/benefit calculus that we face." – DB-J

Re-identification Demonstration Attack Summary

- What can we conclude from the empirical evidence provided by these 11 highly influential re-identification attacks?
  - The proportion of *demonstrated* re-identifications is extremely small.
  - Which ***does not imply data re-identification risks are necessarily very small*** *(especially if the data has not been subject to Statistical Disclosure Limitation methods)*.
  - But with only 268 re-identifications made out of 327 million opportunities, Ohm's "Broken Promises" assertion that *"scientists have demonstrated they can often re-identify with astonishing ease"* seems rather dubious.
  - It also seems clear that the state of "re-identification science", and the "evidence", it has provided needs to be dramatically improved in order to better support good public policy regarding data de-identification.

Appendix

The following slides provide additional details

References for Re-identification Attack Summary Table

1. Sweeney, L. k-anonymity: a model for protecting privacy. International Journal on Uncertainty, Fuzziness and Knowledge-based Systems, 10 (5), 2002; 557-570.
2. Barth-Jones, DC., The 'Re-Identification' of Governor William Weld's Medical Information: A Critical Re-Examination of Health Data Identification Risks and Privacy Protections, Then and Now (July 2012). http://ssrn.com/abstract=2076397
3. Michael Barbaro, Tom Zeller Jr. A Face Is Exposed for AOL Searcher No. 4417749. New York Times August 6, 2006. www.nytimes.com/2006/08/09/technology/09aol.html
4. Narayanan, A., Shmatikov, V. Robust De-anonymization of Large Sparse Datasets. Proceeding SP '08 Proceedings of the 2008 IEEE Symposium on Security and Privacy p. 111-125.
5. Kwok, P.K.; Lafky,D. Harder Than You Think: A Case Study of Re-Identification Risk of HIPAA Compliant Records. Joint Statistical Meetings. Section on Government Statistics. Miami, FL Aug 2, 2011. p. 3826-3833.
6. El Emam K, et al. De-identification Methods for Open Health Data: The Case of the Heritage Health Prize Claims Dataset. J Med Internet Res 2012;14(1):e33
7. Valentino-DeVries, J. May the Best Algorithm Win… With $3 Million Prize, Health Insurer Raises Stakes on the Data-Crunching Circuit. Wall Street Journal. March 16, 2011. March 17, 2011 http://www.wsj.com/article_email/SB10001424052748704662604576202392747278936-lMyQjAxMTAxMDEwNTExNDUyWj.html
8. Narayanan, A. An Adversarial Analysis of the Reidentifiability of the Heritage Health Prize Dataset. May 27, 2011 http://randomwalker.info/publications/heritage-health-re-identifiability.pdf
9. Narayanan, A. Felten, E.W. No silver bullet: De-identification still doesn't work. July 9, 2014 http://randomwalker.info/publications/no-silver-bullet-de-identification.pdf
10. Melissa Gymrek, Amy L. McGuire, David Golan, Eran Halperin, Yaniv Erlich. Identifying Personal Genomes by Surname Inference. Science 18 Jan 2013: 321-324.
11. Barth-Jones, D. Public Policy Considerations for Recent Re-Identification Demonstration Attacks on Genomic Data Sets: Part 1. Harvard Law, Petrie-Flom Center: Online Symposium on the Law, Ethics & Science of Re-identification Demonstrations. http://blogs.harvard.edu/billofhealth/2013/05/29/public-policy-considerations-for-recent-re-identification-demonstration-attacks-on-genomic-data-sets-part-1-re-identification-symposium/
12. Sweeney, L., Abu, A, Winn, J. Identifying Participants in the Personal Genome Project by Name (April 29, 2013). http://ssrn.com/abstract=2257732

References for Re-identification Attack Summary Table

13. Jane Yakowitz. Reporting Fail: The Reidentification of Personal Genome Project Participants May 1, 2013. https://blogs.harvard.edu/infolaw/2013/05/01/reporting-fail-the-reidentification-of-personal-genome-project-participants/
14. Barth-Jones, D. Press and Reporting Considerations for Recent Re-Identification Demonstration Attacks: Part 2. Harvard Law, Petrie-Flom Center: Online Symposium on the Law, Ethics & Science of Re-identification Demonstrations. http://blogs.harvard.edu/billofhealth/2013/10/01/press-and-reporting-considerations-for-recent-re-identification-demonstration-attacks-part-2-re-identification-symposium/
15. Sweeney, L. Matching Known Patients to Health Records in Washington State Data (June 5, 2013). http://ssrn.com/abstract=2289850
16. Robertson, J. States' Hospital Data for Sale Puts Privacy in Jeopardy. Bloomberg News June 5, 2013. https://www.bloomberg.com/news/articles/2013-06-05/states-hospital-data-for-sale-puts-privacy-in-jeopardy
17. Yves-Alexandre de Montjoye, César A. Hidalgo, Michel Verleysen, Vincent D. Blondel. Unique in the Crowd: The privacy bounds of human mobility. Scientific Reports 3, Article number: 1376 (2013) http://www.nature.com/articles/srep01376
18. Anthony Tockar. Riding with the Stars: Passenger Privacy in the NYC Taxicab Dataset. September 15, 2014. https://research.neustar.biz/2014/09/15/riding-with-the-stars-passenger-privacy-in-the-nyc-taxicab-dataset/
19. Barth-Jones, D. The Antidote for "Anecdata": A Little Science Can Separate Data Privacy Facts from Folklore. https://blogs.harvard.edu/infolaw/2014/11/21/the-antidote-for-anecdata-a-little-science-can-separate-data-privacy-facts-from-folklore/
20. de Montjoye, et al. . Unique in the shopping mall: On the reidentifiability of credit card metadata. Science. 30 Jan 2015: Vol. 347, Issue 6221, pp. 536-539.
21. Barth-Jones D, El Emam K, Bambauer J, Cavoukian A, Malin B. Assessing data intrusion threats. Science. 2015 Apr 10; 348(6231):194-5.
22. de Montjoye, et al. Assessing data intrusion threats—Response Science. 10 Apr 2015: Vol. 348, Issue 6231, pp. 195
23. Jane Yakowitz Bambauer. Is De-Identification Dead Again? April 28, 2015. https://blogs.harvard.edu/infolaw/2015/04/28/is-de-identification-dead-again/
24. David Sánchez, Sergio Martínez, Josep Domingo-Ferrer. Technical Comments: Comment on "Unique in the shopping mall: On the reidentifiability of credit card metadata". Science. 18 Mar 2016: Vol. 351, Issue 6279, pp. 1274.
25. Sánchez, et al. Supplementary Materials for "How to Avoid Reidentification with Proper Anonymization"- Comment on "Unique in the shopping mall: on the reidentifiability of credit card metadata". http://arxiv.org/abs/1511.05957
26. de Montjoye, et al. Response to Comment on "Unique in the shopping mall: On the reidentifiability of credit card metadata" Science 18 Mar 2016: Vol. 351, Issue 6279, pp. 1274

References for Re-identification Attack Summary Table

27. Nate Anderson. “Anonymized” data really isn’t—and here’s why not. Sep 8, 2009 http://arstechnica.com/tech-policy/2009/09/your-secrets-live-online-in-databases-of-ruin/
28. Sorrell v. IMS Health: Brief of Amici Curiae Electronic Privacy Information Center. March 1, 2011. https://epic.org/amicus/sorrell/EPIC_amicus_Sorrell_final.pdf
29. Ruth Williams. Anonymity Under Threat: Scientists uncover the identities of anonymous DNA donors using freely available web searches. The Scientist. January 17, 2013. http://www.the-scientist.com/?articles.view/articleNo/34006/title/Anonymity-Under-Threat/
30. Kevin Fogarty. DNA hack could make medical privacy impossible. CSO. March 11, 2013. http://www.csoonline.com/article/2133054/identity-access/dna-hack-could-make-medical-privacy-impossible.html
31. Adam Tanner. Harvard Professor Re-Identifies Anonymous Volunteers in DNA Study. Forbes. Apr 25, 2013. http://www.forbes.com/sites/adamtanner/2013/04/25/harvard-professor-re-identifies-anonymous-volunteers-in-dna-study/
32. Adam Tanner. The Promise & Perils of Sharing DNA. Undark Magazine. September 13, 2016. http://undark.org/article/dna-ancestry-sharing-privacy-23andme/
33. Sweeney L. Only You, Your Doctor, and Many Others May Know. Technology Science. 2015092903. September 29, 2015. http://techscience.org/a/2015092903
34. David Sirota. How Big Brother Watches You With Metadata. San Francisco Gate. October 9, 2014. http://www.sfgate.com/opinion/article/How-Big-Brother-watches-you-with-metadata-5812775.php
35. Natasha Singer. With a Few Bits of Data, Researchers Identify ‘Anonymous’ People. New York Times. Bits Blog. January 29, 2015. http://bits.blogs.nytimes.com/2015/01/29/with-a-few-bits-of-data-researchers-identify-anonymous-people/

Additional Re-identification Attack Review References

1. Khaled El Emam, Jonker, E.; Arbuckle, L.; Malin, B. A systematic review of re-identification attacks on health data. PLoS One 2011; Vol 6(12):e28071.
2. Jane Henriksen-Bulmer, Sheridan Jeary. Re-identification attacks - A systematic literature review. International Journal of Information Management, 36 (2016) 1184–1192.