Martin Nemzow
2915 Flamingo Drive
Miami Beach, FL 33140
305 538-4994 work

Wednesday, December 15, 2010

Ladies and Gentlemen:

I am an expert on security and privacy. I have knowledge of PII exploitation using semantic aggregation used to force reindentification with generic information. I have attached a paper for general consumption.

The *Wall Street Journal's* ongoing series on privacy since August 2010 shows some of the more obvious attempts to own our lives. The various privacy bills sponsored do provide benefits over the many state data breach laws but fall short in so many ways because they are bandaids to a definitional and technical problem. ID theft, misuse, and fraud is clearly a hot button for your constituency. DATA might pass the Senate. I hope it does. Although there are a lot of wrong verbiage, it is a single national law. But, more needs to be done with technical details to be learned. See the attached paper that I hope is simple and clear enough to touch on the many issues. I am in touch with many people who lobby on ID theft issues and promote my paper too. Data breach is not privacy and privacy is not security. Privacy is something different and important if we want to protect our children and future generations. Any new draft will require explicitly worded legislation to reflect technology and operations if you are to curb the abuses and provide venues for enforcement not reflected in prior legislation or proposals.

Thank you.

Sincerely,

Martin A. Nemzow

Martin Nemzow

Requiring Personal PII Ownership

Laws need to change to reflect that a likeness of a person is also reflected in PII too. I need the legal right so that I personally own my own PII, can choose how it is used, who has it or doesn't, and control all references to it. PII is *personally identifiable information*, a fact and fact set that uniquely define each person. PII includes social security number, name, driver's license, address, telephone number, physical attributes, relatives, functional histories, medical diagnosis, email address, a signature and other types of biometric markers. PII is also the fact set that I live in zip code 02145 in a yellow colonial brick house held in mortgage by BankBoston, which can deductively disclose me or establish a subset of matches including me. It defines me as an unique individual, and you too, by way of your own unique PII. My PII is information that is commonly used without recognition that it belongs to me, that I own it, that it is of me in spite of laws that let usage default to aggregators. This PII is about me, part of me, defines me, establishes my likeness, and characterizes my life. It should belong to me but doesn't. Yours should belong to you too.

PII is also reflected by PHI (where the 'H' is 'health') and numerous other references to information in raw data forms, as images, as scanned office notes, and financial or property transactions. Photographs, ancestral records, lists of neighbors, references to friends, aerial photographs, property and taxation records, and other day-to-day events create both a public and private trail in most cases not defined by any laws yet but sometimes part of a tug-of-war over conflicting regulations. While social networking sites like Facebook outwardly reflect the worst in PII privacy, the reality is less obvious channels accumulate the information detritus of our personal lives without redress or control.

Legislation like the MA resident data law[1] includes substantial holes. The MA breach legislation might be a leading law meant to intimidate data aggregators, but what is really scary are the presumptions about PII, ownership, and even technology not reflected by rigorous legalese. This law presumes that information is owned by an 'individual' meaning in this context the aggregator as information collector. It is a poor choice of terms that will certainly result in challenges. This ownership assertion is a slippery issue when most data integrators are legally defined as corporations, and only one of many flaws apparent in my reading. As a consequence, the individual that owns the data is not the individual about whom the data describes but rather the aggregator. These definitions are clueless without defining clear rights of parties, what PII is, or aggregations implying deductions that might skirt PII regulations.

In fact, we let aggregators have these rights, for free, without reservation. Until a fundamental right for PII ownership is legislated, the many issues of data breaches, ID thefts, invasion of privacy, and right to a quiet enjoyment will remain without hope of clarification now or as technology evolves. I need rights to balance threats to privacy. I need unequivocal personal ownership of my PII.

Privacy will not be possible until legislation defines who owns PII and what it functionally is. As it stands, I do not really own the usage of my own name, the reference to where I live, or cookie crumbs of information used in part or in aggregate to paint who I am. As long as usage of my name is not fraud, malice, defamation, libel, or slander it is free to use. I have limited ability to correct false information; even less chance to have it purged from companies tracking me unbeknownst to me. Additionally, some companies claim my information posted on government or open websites reflect the public domain whether I authorized the use of my information or not. These aggregators assert all rights to use my public digital PII likeness as they please. My PII information resides in databases of aggregators that I do not know, that resell some or all of my information in ways often detrimental to me.

I assert that aggregators are only custodians. I should be the owner, and by rights it is about me, by me, for me, and represents my legal likeness. How could they own part of me without remuneration to me or my say in some implicit contract? Some might assert there is a social contract for the public and commercial usage of PII, but if so, it is so full of holes and historical mistakes that we need to formally fix it. It is a bad social contract that needs to be voided. I need a new social contract restoring me to me.

---

[1] http://www.mass.gov/Eoca/docs/idtheft/201CMR1700reg.pdf

I need to have a say in who has my information, notification that someone or anyone or everyone has accumulated my information so I can reclaim it, assert rights to how it is used, and control what is essentially my likeness. I need an evolving description of PII and a statistical description of how details aggregated can jeopardize my privacy or deductively disclose who I am from my cookie crumbs not even seen as PII. I need to know that my name is mine, my signature is mine, any 'wallet' of legal or incidental identification is mine alone. I need power to claim that open usage of single or aggregate information reflecting my PII is a violation of my privacy. I need control to remove it from data collectors unregulated by much of anything. If I provide my information to create a mortgage, that information is let for that specific use and not bartered ever after for secondary advertising or resale in ways never considered. I need a restriction that protects me from changes in technology so that unforeseen repurposing of my PII cannot take away my rights to me that might not have been even a concept when I first applied for a mortgage. I don't want to be able to sell my birthright except with the known and understood consequences at the time should I sell such a right. I should retain legacy rights to my identity should I choose to reclaim it. PII should not be a trick that is too complex for the average person.

Of primary concern, I want to be able to trace the derivation of such information used in ID theft against me and hold aggregators accountable for disruptions and damages. I want legal standing primarily in my residence county for all breaches, both local and enabled by the Internet and other technology that imparts the intangibility of information to be anywhere. I want to have the right to sue against far-away assailants that by usage of my information are bound into me and my residence county under local legal jurisdiction. If I win, I want to be able to preclude such assailants from doing business again in my county if they fail to conform to my judgment or injunction as pressure to abide by these laws. The consequences of violating my PII and my likeness should not be so intangible as to allow the bad guys to sidetrack local legal domains with impunity. Bad actors should not be able to pull up stakes and repeat these scams. More importantly, I do not want my PII stored and used under rules of any foreign country or out in space. The MA data breach legislation at least pulls back domain to something tangible and actionable.

My rights with my PII should be with me and where I am, not in the fictions of cyberspace and other international communications channels. I clearly do not have such standing, but if privacy and my rights to own my PII are an essential right, tough definitions, clear ownership, and rights to contract need to be part of new laws with local transparency and enforcement. I do not want to and cannot afford to personally fund judicial activity to establish a precedent that PII is a likeness that I have under common law. Instead, I want the legislators to do their jobs creating a functional privacy basis. I have been victimized with information from 20 years ago posted for ways well-intentioned and allowed under 'Sunshine Laws' but clearly violating other FL laws and Federal laws. I cannot access legal venues without pockets deep enough to support an entire law firm. Laws clashing with other laws are generally settled by legislatures or appellate courts, venues beyond my means but well within the war chests of aggregators and the well-paid lobbyists representing them. It is an unequal fight, starting from an unequal basis of a twisted social contract ceding most rights for my PII to the aggregators instead of to me. Return my good name to me. It shouldn't have to lease my own name from a broker or pay just to see it. It is mine, so I want it back. Do you want yours too?

Obviously, there are limitations to PII and a social need for it to be aggregated, like credit reporting or law enforcement. There will be complications. I will want the highest credit score, a clean criminal record, and favorable information in such reports whether true or not. Others instead want accuracy. As such, the information still needs to be mine, with the consequences for the information and how it is used still under my control. If I want to lose the benefits brought by credit reports, then it should be my choice too. I should have say in the scope of its distribution. I can control how my face is used in movies or choose not to show it; likewise, I should be able to control my PII and its ensuing likenesses with control over the social and economic benefits through its personally contracted distribution.

But a social or economic need should not mean my medical prescriptions can be sold to data aggregators who use it to redline me from new mortgages, set my car insurance rates, or decide that I might be an unreliable employee. As it is now, my certified requests to find out under current laws whether Walgreens and CVS have sold my Lipitor records have remained answered, although MediScape the aggregator show such transactions. I also know drug reps get lists of patients and prescribing physician sold by these

pharmacies, sometimes badly anonymized and other times fully in the clear. I have received these lists about me (sometimes about other people) accidentally mailed to me but clearly not intended for me. There will be tensions between private rights and social needs, but these can be resolved in a more structured way than 50 states trying to define data breach laws against evolving technological innovation. Big businesses with a stake in the profits from new laws lobby against personal interests, like economic, health, lifestyle, and predictions, all aggregated forms of my PII I want to reclaim and control.

The ownership of PII, the uses to which PII can be used, and data breach by custodians are distinct issues not to be confused by coverage of a single partial law reflecting the ambitions for all. Current data breach laws reflect the consequence of loss, and in some cases, requirements for security. They do not define the types of PII or explore the consequences of aggregation creating alternate PII or assignment of functional codes to reestablish links to me that technically skirt existing law. These laws frequently do not establish what constitutes a loss or partial loss as an improper release of information in a wide range of situations that represent misuse rather than simple exposure. These laws frequently do not establish the consequences when information is aggregated without actual breach but still causing problem for persons impacted. Common law is about less rigid interpretation, something essential for reconstructing a social contract for PII that restores mine to me, and yours to you.

There is also a tension in the security of this PII, one that is not finding traction. If I have no faith in aggregators to protect my information, I want to recall what they have and take it away from all subordinated custodians. Even the military with unlimited budgets cannot establish an effective baseline for security; they suffer ignominious breaches every day. The security they have is out of price range for businesses and yet does not work. Data aggregators do not have such resources or ever will, so the technology for security seems endlessly beyond any grasp. They have no economic incentive to protect my PII. Loss is perceived as a business risk, which in the terminal case is only as large as bankruptcy, small consolation after many breaches against me. Attempts to legislate penalties for theft lack everything. Even $250,000 per instance HIPAA penalty has not stemmed losses. Name a single prosecution. These are toothless laws with only the Federal AG in the office of EEOC possessing standing to file suit. If these laws cannot protect my info, I want it back now. Give me back mine to me. I want to choose how I let my PII be used, stored, risked, or even not at all. I would think you want yours too.

Fundamental definitions are required to reflect the complexity of ownership, custodianship, and rights and responsibilities due each party. A chain of custody is a weak link when information is sold, but is probably necessary to hold subordinated custodians responsible for violations. I do not know who has my PII even as a direct result of transactions I initiated. I certainly do not know where this information has gone. I would like to qualify its benefits and risks to me, track breaches, or most likely recall this information for my safety given the awful state of data security and my understanding in ways in which aggregated but not PII under categorical definition can be combined to expose my secrets or paint an unflattering likeness of me. This would give me rights for personal enforcement and even the ability to audit what is held and how safe it is without reliance on police actions. I want laws in depth to reflect the rigor required to define PII, ownership, custodianship, and penalties available to me when my PII is misused.

I assert that a legal basis for PII was defined in the seminal "The Right to Privacy," in *Harvard Law Review* article by Samuel Warren and Louis Brandeis in 1890.[2] This paper extended common law rights for privacy into new areas as audio and photo recordings were becoming widespread. In a similar extension of rights, I need my PII to reflect my digital likeness and have legislative rights to how it is used and rights to make contracts with it too. People can always make stupid contracts and fritter such rights away, but we need to start somewhere. It is not enough to think that privacy is lost and to 'just get over it', as one captain of industry, Scott McNealy, preached.[3] It is a practical response to the issues but not be an acceptable one to me. Basic legal structures for privacy are in fact in place; our politicians and judges need to close loopholes. Privacy is lost only if we abdicate rights to it. Get over any thought of accepting a bad social contract. PII is still mine -- and yours -- if we forge a better social contract for privacy with PII.

[2] http://www.law.louisville.edu/library/collections/brandeis/node/225
[3] http://www.wired.com/politics/law/news/1999/01/17538

Warren and Brandeis express that the individual "retains the power to fix the limits of publicity" (for photo and audio) and this should be extended to PII to reflect technical evolution and the "ability to prevent publication at all" and "to be protected in the exclusive use" of PII. These authors also acknowledge the flexibility of expression without limits to form recognizing that "signs" reflect meaning and damages unforeseen and therefore to be protected in all forms, not limited to copy, semblance, or catalog.

Laws for breach notification are examples of locking the door after failure. It is delayed response rather than an effort to understand and regulate all types of data resource before misuse. Such laws presume without formal legislation that PII belongs to the aggregator. Any belief that PII belongs to aggregators is just a mistake of a weak social contract that we continue to allow. It is a consequence of default when business establish de facto rules for its own benefit. Regulation reflects specifics of data aggregation and storage, not the fundamental issues of why we let all the power to the aggregators who clearly do not have the power to control the burgeoning consequences of security lapses. It is high time to reconsider that. It is no longer a niche market but a fundamental cog in the information revolution. Regulation no longer works and distorts the future that should not unfold without a privacy contract and ownership rights to PII.

PII after death will need to be defined too, perhaps naturally accruing to heirs. This will suppress some of the subterfuge with creating IDs from dead people and insurance scams for people omitted from the SS death index. Obviously, twins and other multiples, people with innocently overlapping PII represent special definitional cases. But these examples reflect the consequence that a likeness is not just a single fact like the SSN but an aggregation that will reflect another person with variations. As such, the definition of PII cannot be as lame-brained as the HIPAA fair harbor categories. It must reflect generic methods for information not specific alone but combined to uniquely describe each individual within the population. A breach can happen when information about an unique individual is incorrectly asserted to a wrong relative. For an example of aggregation, birth stone and current age are anonymized information about an individual that together establish month and year of birth. When a name is used in a lookup, partial date is easily confirmed with exact date establishing an unqualified breach of security. Just 12 bits out of 33 seems enough for inference to effectively breach any legislated definition of PII without legally violating any extant law.[4] There will also be issues of PII that change naturally or is intentional altered, such as hair color, weight, tattoos, with how they relate to legal definitions.

Similarly, DNA is a marker with limited protection. This is just one of many aspects of PII in flux. We will not understand the consequences for years to come and can only imagine some violations of ownership and loss of privacy. My blood taken for routine physical sent to a lab can be screened without my knowledge for any number of genetic diseases or for a full profile. It could be used for purposes I cannot yet imagine and patented with no benefit to me and risk to my heirs. It is my PII, but not my right to own. I might share it with others, but it should still be a likeness of me with my rights to it alone or for whom I choose, such as my offspring. Although a full DNA profile is now $48K, it was $10M just a few years ago. In a few years, the information might cost a handful of dollars. As technology advances I can foresee kits to clone DNA and use it fake the forensic evidence for a crime.[5][6] As outlandish as this might all seem the consequences of aggregation were unknown to Brandeis and Warren but now disruptive in ways still unimaginable.

My PII is my likeness. I want Congress to stand up to define PII, all its current varieties, all the forms that can aggregate to a likeness. I want Congress to formally restore my own rights to me. I want Congress to formally restore your rights to your own PII to you. Other issues of security come later, but data breach laws are flagging behind accelerating technology and only one hot button in lapse and loss of information security. There is a big disconnect in the social contract and gaping loopholes in this new private property with serious consequences and far-reaching implications. It is appropriate to return the incentive for control to the party with the vested interest in my PII, which is me, or your PII, which is you.

---

[4] http://www.eff.org/deeplinks/2010/01/primer-information-theory-and-privacy
[5] http://www.nytimes.com/2009/08/18/science/18dna.html
[6] http://www.fsigenetics.com/article/S1872-4973(09)00099-4/abstract