Reasonable Expectations of Privacy Indicators

Erin Kenneally

International Computer Science Institute
Berkeley, CA, USA
erink@icsi.berkeley.edu

U.S. Department of Homeland Security;
Washington, DC
Erin.Kenneally@hq.dhs.gov

ABSTRACT

The incumbent approach to defining our reasonable expectations of privacy (REP) fails to account for the evolved threats ushered by the Internet context. As a result, the privacy controls it anchors are being applied in an inconsistent, ad hoc, and precarious manner.

This paper briefly introduces a novel approach to domesticate REP and operationalize its application through privacy controls by taking cues from the playbook of network science. This approach re-conceptualizes information privacy as a scale-free network that follows power law dynamics, and it suggests gauging privacy risk by looking at the nature and quality of links and nodes controlling personal information artifacts rather than whether the interface to data is deemed public or private.

Conjecturally, the resulting privacy framework will achieve balance between individual rights protection and public good goals by advocating a regime of reciprocal obligations between the countervailing interests: the recognition of a more nuanced privacy continuum by private information controllers and more overt manifestations of REP by privacy subjects, both steeped in a network theory-informed understanding of information flows.

1. INTRODUCTION

Data privacy is an evolution of control tug-o-war between individual rights and interests, social responsibility, and innovation. When users overtly interact with or passively engage a website, social networking or otherwise, they enter a privacy risk zone. Most often, they cannot be sure whether data is surreptitiously being collected, will be used, or further disclosed in ways that contravene their privacy preferences. While we have evolved the 'state of the art' to obligate sites to disclose their privacy collection, use and disclosure policies, protections nevertheless hinge on ex ante user trust that websites and online entities will walk the talk.

A privacy solution steeped in information use[1] restrictions and obligations can be approached by better engineering the identification and application of the underlying *reasonable expectations* upon which our privacy controls (laws, policies, standards) operate. This paper posits that the information privacy risks and interests that comprise these reasonable expectations flow similar to scale-free information communication networks. An effective privacy strategy, therefore, may be derived from the nature of the space creating the problem to begin with. Specifically, a scale-free problem demands a solution derived from scale-free network science.

2. Problem and Solution Overview

It seems intuitive that privacy harms are not tied to whether you're at home, or in a park, with a crowd, or in a public phone booth -- yet the trigger for whether we have a reasonable expectation of privacy (REP) is still largely tethered to the contours demarcating public-private *realspaces*. In general, if one's behavior is conducted in 'private' then REP attaches, but if it is exposed to the 'public' then surveillance, tracking, collection, and use of that information is fair game. How do we play the game, however, when our privacy is tethered to information that is decoupled from our persons across the networked ecosystem that does not intuitively fall along public-private boundaries?

The law has not kept pace with the exponential evolution of technological capabilities and accompanying social changes, causing arguably unprecedented privacy risks. Information privacy is an evolution of control tug-o-war between individual rights and interests, social responsibility, and innovation. The divergence between expectations and capabilities is manifest at the crossroads of electronic data protection and security, e-commerce, online social networking, and law enforcement and infrastructure protection where fundamental notions of privacy and identity are shifting. It is here that the principle of "reasonable expectation of privacy" has become unmoored from traditional controls -- laws, policies, private agreements and standards – because those are steeped in old paradigms from the non-network environment. Consequently, institutional and individual privacy risk management approaches that take cues from ill-fitting models demand new girders.

We lack a consistent, objective measurement for assessing reasonable expectation of privacy and need to realign standards and their applications to more empirically reflect the contours of the network environment in which the privacy risks occur and privacy interests need protection. This paper proposes a new way to domesticate REP using models from network science. In order to move beyond the circular paradigm where our privacy controls apply REP by what is deemed 'private' and vice versa, we need a model that organically measures REP based on the capabilities and risks in the cyber environment, and one that allows those new metrics to inform a reshaping of our privacy controls. Modeling information privacy as a scale-free network may enable a more tailored understanding and prescribing of the conditions necessary

[1] "Use" is meant broadly to encompass publication, dissemination, and disclosure.

for a privacy control regime to succeed. Stated differently, if privacy risks and interests flow with the PIA vis-à-vis a scale-free network, this model promises to inform a better application of privacy controls.

This paper approaches this problem from the conceptual strategy that information privacy is a complex adaptive system. Other legal scholarship has applied this strategy to legal contexts such as environmental policy, telecommunications policy, intellectual property law, common law jurisprudence, Internet jurisdiction, and information privacy torts. This approach advocates the novel application of network science to a broader value that underpins many of our privacy controls- reasonable expectation of privacy. It posits that there is a co-evolution between privacy controls (laws, regulations, standards) and informal norms. From this position, REP is both a bottom-up and top-down tenet, where social norms of what citizens should reasonably expect to be afforded privacy protection should influence our controls, and our controls should shape our REP. As such, an information privacy regime that is predominated by the latter, governance-imposed notion of REP does not objectively reflect the reality of REP 'in the trenches' and threatens to institutionalize a fiction that results in inefficiencies and disrespect for ordering forces that protect individual rights and fosters social good and innovation.

We can infer the incongruity between legacy-driven measures of REP and the changed normative expectations wrought by the Internet environment from contemporary controversies surrounding online social networking, geo-location based services, targeted behavioral advertising, and data anonymization. Using a network science model, we may be able to harmonize the understandings and applications of REP across associated privacy controls such as the 4th Amendment, ECPA, FOIA, self-regulatory standards, consumer protection regulations, privacy torts, civil discovery rules, and private contracts and policies. Finally, network science techniques may enable us to operationalize REP into a more predictable, coherent, empirical framework for descriptive evidentiary proof and prescriptive risk management.

3. Problems with the Old Playbook

Thresholds for privacy protections are anchored around the `reasonable expectation' principle that explicitly or implicitly underpins institutional privacy controls- laws, regulations, industry standards, and private agreements. The incumbent standard for measuring and applying REP is obsolete and contemporary cases and controversies shine light on our need for a new model. This legacy is largely anchored in the delineation between public and private spaces (closely related is the third-party doctrine), which broadly holds that what one knowingly exposes to the public loses any expectation that it is deserving of protection under the law.

This distinction is built on a spatial and temporal reality of offline physical spaces where privacy interests were exerted and harms occurred, e.g. clear delineations between public and private spaces steeped in what one could contour dominion around such as one's home, body, and personal effects. In other words, historically, the level of privacy protection depended in large part on place. Indeed, privacy attachment migrated rightly from the space occupied by a person to the person proper, but nonetheless it maintained an anchor to the nature of the space. Our networked information age begs further evolution of REP to encompass personal information artifacts (PIA) as a direct extension of the person, the challenge being that information is often decoupled in both time and space from the person asserting the right.

We have defined what public-private means with respect to a person's location, property and behavior, but with regard to his information in an online social network space, the legacy metrics are exposed by unresolved cases and controversies as too coarse and unreflective of the nature of the threat to the underlying privacy interest. Our privacy expectations --the interests and rights associated with relationships between persons with respect to the collection, use and disclosure of data -- are informed by controls (laws, policies, standards) whose measurements and applications of privacy are ill-fitting given the information privacy threat model.

The application of REP in our network environment is a holdover from legal protections which itself was derived from a REP born and matured in a different environment. This legacy playing field is dictated by a mechanic Newtonian physics-oriented playbook, whereby our norms and expectations flow directly from everyday sentient activities, and we anchored public and private boundaries for naming and protecting against risks. Even with regard to ephemeral information, realspace privacy norms co-evolved amidst a default where it was comparatively easy to destroy information and hard to make copies. This new 'playing field' does not have those temporal and spatial boundaries around which public and private was demarcated.

With those time-space boundaries largely eliminated in the cyber context, we discover different capabilities and risks that in turn inform our expectations for what deserves protection. This has catalyzed an arguable collective cognitive dissonance over our privacy expectations. Our traditional legal control structures draw expectations for what is reasonable to have privacy in based on measurements that are perverse in the network context -- we are using the public-private metric (sometimes taking the form of third party exposure) to determine privacy risk. Yet, the capabilities and risks we experience push back expectations for what deserves privacy protection that do not map to the public-private gauge. Metaphorically, we are trying to use a sundial to manage the Boston Marathon when what we need is chip timing.

In short, we are being lead by REP indicators (i.e., public-private) from a legal structure that originated within a fundamentally different capability and risk paradigm.

3.1 Fractures Manifest

The incumbent REP approach may be faulty because it lacks contemporary contextual acumen – i.e., the conditions of information collection, use, and disclosure that reflect the Internetwork playing field for information privacy. As described in the next section, the current REP paradigm is fundamentally contoured around public versus private measurements that presume a scaled network of information flows where every PIA controller (PC) is equivalent. PIA Controllers refer to the persons or entities – third parties or data subjects themselves – who possess and have the capability to disclose PIA. It predominantly treats all disclosures to third parties identically rather than framing privacy risks empirically according to the fitness of and scale-free relationships between PC, and thereby sets the stage for incongruous protection and enforcement of rights.

Before delving into the implications of a scale-free model on information privacy, it may be helpful to illustrate where the

incongruity between our REP and its measurement and protection is manifest. Popularized cases and controversies offer a window into the tension between emerging REP norms and legacy privacy controls.

3.2 Location, Online Social Networking and the Fourth Amendment

The definitional confusion in determining REP in the Internet communications context, using indicators such as whether the data was in a public-vs-private space, has led to cognitive dissonance over expectations of rights and protections afforded to data, which circumstances trigger those protections, and whether in practice those protections are invoked. Examples include the controversial Google Street View case, discord among federal appeals courts over geographic location information, and the legal grappling over the privacy of social networking information. There is uncertainty to what extent REP attaches to the wires or airwaves carrying Internet data, as well as to certain Internet data itself like GPS, Internet Protocol Address (IPA) and Uniform Resource Locator (URL) because relying on whether these are disclosed to the public-vs-private are not accurate indicators of privacy threats and normative expectations.

Whether there is a reasonable expectation of privacy is a threshold question for invoking constitutional privacy rights protection under the 4th Amendment. The trigger is whether the government must have engaged an *unreasonable search*[2], which turns on whether there is REP in the item searched. The Electronic Communications Privacy Act (ECPA), our statutory implementation of the 4th Amendment for electronic communications, similarly binds privacy protection to REP that often turn on the public-vs-private indicator. A lack of REP implicitly precludes ECPA liability insofar as it is not illegal to obtain network traffic that is accessible to the public.

Whether there is REP in cell-site location information (CSLI) is the latest legal battle related to defining privacy indicators for location data. *U.S. v. Graham* reversed a prior ruling in concluding that there was no REP in historical CSLI and the government does not violate the 4th Amendment protection against unreasonable searches and seizures when it collects that information without a probable cause based warrant.[3] This Fourth Circuit ruling is consistent with the trend in case law.[4] The line of reasoning is based on the longstanding precedent that there is no REP in information voluntarily exposed to a third party, which is arguably a variant of the public-vs-private measure. Graham indicated that the very disclosure of CSLI to Sprint negated any reasonable expectation of privacy. Given that the disclosure of metadata/non-content data like CLSI is prerequisite to the provisioning of services, delivering of communications, and fulfilling of transactions by third parties on the Internet, it is unsurprising that the using exposure to third parties as a REP indicator is increasingly contested. The Graham court hinted at the problem posed by technology to privacy in light of this doctrine by suggesting that Congress can step in to make sure privacy does not become a 'casualty of technological progress', as was the case with wiretapping and ECPA.

When it comes to other location information, privacy indicators for GPS data acquired via government tracking seems to have evolved to be more aligned with normative REP. At one point the circuit courts were split over whether the warrantless use of GPS to track public behavior or collect public data over time violated REP. But, the Supreme Court clarified in U.S. v. Jones that the Government's installation of a GPS device on a target's vehicle and its use of that device to monitor the vehicle's movements, constitutes a Fourth Amendment search.[5] Since Jones reached this conclusion by relying on physical trespass, the question of whether there is REP in GPS tracking data that is obtained electronically is not definite.

US v. Maynard[6] is instructive in this regard. In finding that police GPS surveillance was unlawful, it reasoned that tracking of the subject's movements continually across time, thereby "discovering the totality and pattern of his movements from place to place to place," violated his REP. Here we start to see how the traditional REP indicator, public-vs-private, is being modified to include an element of time such that while short-term monitoring of a person's location and movement on public streets would not violate REP, monitoring across time would. This is important in light of the and the ubiquity of mobile devices embedded with GPS tracking technology, and the upsurge in online behavioral advertising by a scarcely regulated industry,, the issue promises anything but a dormant future.

While GPS surveillance cases highlight the issue of whether we have REP in the recording of our behavior in public over time, the Google Street View kerfuffle raised the issue of whether there is REP in data communicated in the open unencrypted wireless network space. The issue was whether Google violated federal and state privacy laws in deploying packet sniffing technology to observe and collect transactional and communications content from the unsecured network routers while taking pictures in neighborhoods for its Street View program. The U.S. Supreme Court rejected Google's argument that it did not violate

---

[2] The reasonableness of a search depends on the totality of the circumstances, including the nature and purpose of the search and the extent to which the search intrudes upon reasonable privacy expectations. In determining whether a search is reasonable, the Court must "consider first the `scope of the legitimate expectation of privacy at issue,' then the `character of the intrusion that is complained of,' and finally the `nature and immediacy of the governmental concern at issue' and the efficacy of the means employed for dealing with it." *Doe ex rel. Doe v. Little Rock Sch. Dist.,* 380 F.3d 349, 352 (8th Cir.2004) (quoting *Vernonia Sch.* 1142*1142 *Dist. 47J v. Acton,* 515 U.S. 646, 654-66, 115 S.Ct. 2386, 132 L.Ed.2d 564 (1995))

[3] United States v. Graham, 796 F.3d 332 (4th Cir. 2015).

[4] See United States v. Carpenter, Nos. 14-1572/1805, 2016 U.S. App. LEXIS 6670, 2016 WL 1445183, at *4-6 (6th Cir. Apr. 13, 2016); United States v. Davis, 785 F.3d 498, 511-13 (11th Cir.) (en banc), cert. denied, 136 S. Ct. 479, 193 L. Ed. 2d 349 (2015); In re Application of U.S. for Historical Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013).

[5] *US v. Jones*, 132 S. Ct. 945, 565 U.S. 945, 181 L. Ed. 2d 911 (2012).

[6] United States v. Maynard, 615 F.3d 544 (2010).

communications privacy law because open Wi-Fi is like radio communications.[7] [8] So the REP indicator here- communications not readily accessible to the general public- is not always easily applied. How do non-technical users set expectations based on this indicator if it is interpreted based on low level technical understanding and device configuration?

Lastly, on the issue of REP in social media, the *Crispin v. Audigier* court struggled with determining whether a user's wall postings and comments on social networking sites Facebook and MySpace were private and thereby triggered privacy protection under the ECPA.[9] Since REP in those Internet communications was undecided, the court remanded the case to determine if plaintiff's privacy settings on the social networking sites rendered the messages public and outside of the purview of stored communications privacy protections. Years later a district court ruled that Facebook wall posts that are configured to be private are, by definition, not accessible to the general public. SO Facebook wall posts are covered by ECPA because the Plaintiff selected privacy settings limiting access to her Facebook page to her Facebook friends.[10] The takeaway here is that despite the public nature of social media, steps taken by individuals to limit disclosure are used as REP indicators.[11]

Can we render satisfactory determinations about whether airwaves, wires or open file shares are afforded REP by characterizing the space or medium where the information is according to binary public or private indicators? Under that playbook, calling it a public space would establish a default absence of REP, and leave the data traversing it open to surveillance, interception, and disclosure. Declaring it private, conversely, would introduce an expectation that it deserves legal protection and privacy rights and risks would be triggered. However, tapping a wire, sniffing a certain airwave frequency, or automatically downloading files from open shares captures PIA that is both responsive and unresponsive to our normative interests in safeguarding our autonomy, seclusion or property. Doing so, in other words, over-inclusively and under-inclusively protects the privacy interests in the data.

The aforementioned cases and their kin are not unsophisticated in their approach to resolving the issues according to the coarse public-private indicators. But, because of the incongruity between REP and their indicators, decisionmakers reach for more reasoned and granular measure to assess and apply REP, such as efforts to secure the wire or configure website privacy settings. Nonetheless, foregoing the legacy public-private standard may entail a painstaking justification for departing from precedent, contorting the legacy standard to fit what the court deems to be just, and/or applying first principles to resolve novel issues in an ad hoc, inconsistent and inefficient manner.

3.3 Disclosure of Anonymized Information and FOIA, Terms of Service Contracts

Is there REP in anonymized PIA that can be re-identified? Federal FOIA and various state open records counterparts balance individual privacy versus public access to government records by excepting from disclosure certain information that is deemed to not have REP. Refusal to exempt PIA (e.g., name, address, birth date, photograph, height and weight) found on driver's licenses is justified because it lacks REP and therefore has no constitutional protection. Again, this determination is steeped on public-private contours, namely that the PIA is commonly exposed to third parties such as when cashing a check, using a credit card, or buying alcohol; and, that it is available from various other sources.[12]

However, as long as the data is a participant in the Internet ecosystem[13] the identifiability of information is not confined to the bounded space of the entity controlling the data, nor the point in time within which it is safeguarded or functionally obscured, nor even the strictures of efforts to anonymize or obfuscate identity[14]. This dynamic changes the rules of the game such that REP measured by the public or private posture of the PIA does not capture the potential privacy risk. More specifically, the problem with assessing the sensitivity of data (e.g., whether it is personally identifiable) along the contours of exposure to the public, is that the confluence of the increasing quantity and availability of information, and the advanced technical (computation, analytics

---

[7] *Joffe v. Google, Inc.*, 729 F.3d 1262 (9th Cir. 2013).

[8] In addition to the consolidated class action lawsuit, by 2012 more than twelve countries investigated Google for its collection of private Wi-Fi data, and at least nine countries found that Google violated their national wiretap laws; also Attorneys general for 38 states and the District of Columbia reached a $7M settlement with Google over consumer protection and privacy claims; *See*, http://www.ct.gov/ag/cwp/view.asp?Q=520518&A=2341.

[9] *Crispin v. Christian Audigier, Inc.*, 717 F. Supp. 2d 965 (C.D. Cal. 2010).

[10] *Ehling v. Monmouth-Ocean Hosp. Service Corp.*, 961 F. Supp. 2d 659 (D.N.Y. 2013).

[11] *See, e.g., Viacom Int'l Inc. v. Youtube Inc.,* 253 F.R.D. 256, 265 (S.D.N.Y.2008) (holding that SCA prevented Viacom from accessing YouTube "videos that [users] have designated as private and chosen to share only with specified recipients").

[12] For example, *Reno v. Condon*, 528 U.S. 141 (2000), "a State-issued driver's license is often needed to cash a check, use a credit card, board an airplane, or purchase alcohol. We seriously doubt that an individual has a constitutional right to privacy in information routinely shared with strangers."

[13] The practical reality of our network infrastructure and information flows.

[14] *See, e.g.*, Barbaro, M., and T. Zeller, J., A Face is Exposed for AOL Searcher No. 4417749, New York Times (Aug 2006), Narayanan, A., and Shmatikov, V., Robust De-anonymization of Large Sparse Datasets, IEEE Symposium on Security and Privacy (2008), available at http://www.cs.utexas.edu/~shmat/shmat_oak08netflix.pdf, (illustrating notorious examples of anonymized data that was reidentified using publicly-available information).

and transport) capabilities to link these public and private collections mushroom the notion of identifiability to the point of meaninglessness.

Stated differently, the unit of privacy risk assessment has changed and the standard for determining REP must respond in kind. The name and SSN-anonymized e-commerce account, abandoned or partially accurate Facebook profile, or nameless facial image in Flickr, may have a low privacy risk as it resides compartmentalized in the respective databases and web portals. But, the privacy risk is no longer confined to those measurement criteria. Reasonableness dictates that we consider the plausible "mosaics"[15] of information with which the seemingly benign or "public" data can be combined to heighten the privacy risk posture.

Entities implementing disclosure-centric privacy controls such as FOIA, HIPPA, state data breach notification law, and corporate electronic privacy policies are grasping the empirical reality of the privacy risks.[16] Nonetheless, they are doing so without a replicable, coherent methodology for assessing and applying underlying REP that is in tune with the risks of disclosing seemingly anonymized or facially insensitive data. As a consequence, the level of liability risk and scope of their protection obligations is uncertain.

4. A New Playbook Using A Scale-Free Network Model

The social network environment demands an evolved privacy risk management model that correlates to the contours of this new context. Relative to the legacy, offline context of privacy there are certain features of the online setting that render legacy metrics for determining REP unsuitable: there is much less awareness and understanding of the technology underpinning PIA location and movement; the data relevant to privacy interests is continuous and as such privacy choices are not discrete and linear; and, the boundaries that inherently define privacy are now virtual and not sentient, thereby rendering privacy risk more opaque.

Networks are comprised of nodes connected by links. Lay examples include: scientific research paper citations, the sales of books and branded commodities, the World Wide Web, webpage hits, the number of citations on scientific research papers, and certain criminal activity. If information privacy is a scale-free network, it exhibits some fundamental characteristics [Fig1]:

1. The distribution of nodes approximates a power law distribution, where few nodes have many links (aka, hubs) and the majority of nodes have few links.

2. The network evolves and is dynamic, meaning that nodes are added and removed throughout time.

3. Links exhibit preferential attachment, commonly coined as 'the rich get richer,' whereby new links are added to nodes based on either the number of existing links or some measure of fitness of the node.

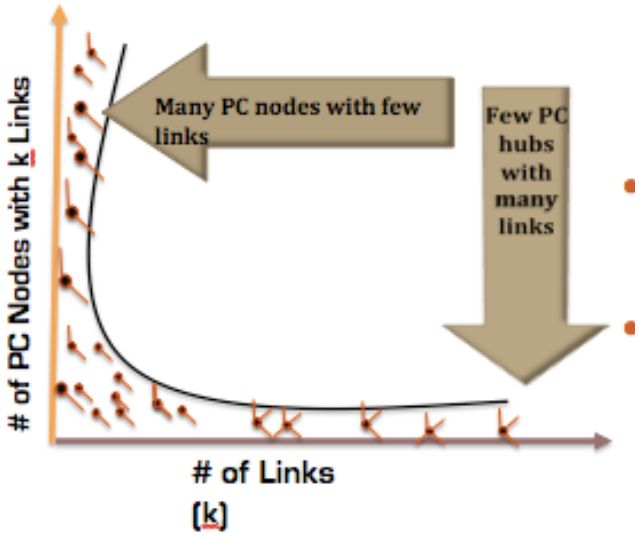

Figure 1: Privacy as a Power Law Distribution

In order to move beyond the circular paradigm where our privacy controls apply REP by what is deemed 'private or public' and vice versa, we need a model that organically measures REP based on the capabilities and risks in the cyber environment, and one that allows those new metrics to inform a reshaping of our privacy controls. Modeling information privacy as a scale-free network may enable a more tailored understanding and prescribing of the conditions necessary for a privacy control regime to succeed. Stated differently, if privacy risks and interests flow with the PIA vis-à-vis a scale-free network, this model promises to inform a better application of privacy controls.

Hypothesizing that we can model information privacy according to the properties of a scale-free network in order to better describe and protect REP means that the nodes are the Personal Information Artifact (PIA) Controllers and links are the collection/disclosure of PIA (the collection, use or disclosure of PIA) between nodes [Fig2.]

---

[15] *See, e.g.*, Pozen, David E., The Mosaic Theory, National Security, and the Freedom of Information Act. Yale Law Journal, Vol. 115, pp. 628-679, 2005. Available at SSRN: http://ssrn.com/abstract=820326.

[16] *See, e.g.*, Southern Illinoisan v. Dept Public Health, 349 Ill.App.3d 431 (IL Sup Ct, 2006) (finding Cancer Registry Data May Be Available Through FOIA because itdid not 'tend to lead to the identity' of patients (and thereby violate the Registry Act) because although the data was readily available to the general public, the identification process was not a simple task that almost anyone with a computer could accomplish); *Department of Justice v. Reporters Committee for Freedom of the Press*, 109 S. Ct. 1468 (1989)(exempting "rap sheets" compiling people's criminal records from FOIA on privacy grounds even though each offense was separately listed in public documents scattered through decades of courthouse files.).

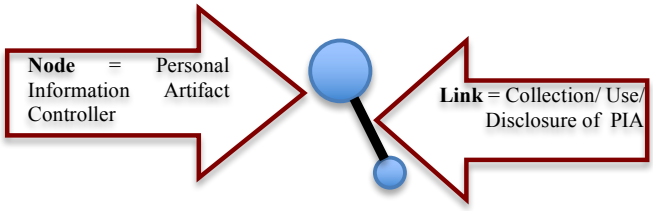

Figure 2.

5. Validating Privacy As a Scale-Free Network

Before we can operationalize an evolved assessment of REP to inform privacy controls using network science techniques, ensuing research needs to validate this approach by exploring the following types of questions:

* How is information privacy like a scale-free network? If so, what does it mean for describing and prescribing REP? For example, what are the possible normative implications for information privacy law, such as whether PIA exposure to 3rd parties is a de facto poor indicator of greater threat to privacy? How might knowledge of PIA flows either eliminate the use of public-private standard for measuring REP; or, can it be used to re-define what we mean by public-private space with a fidelity that is more aligned with the reality of information flows? How well are certain PC integrated with a whole system, such as data aggregators or online advertising networks? How closely does the geo-location of PIA-controller hubs correspond to traditional public-private and 3rd party doctrines? Will the model challenge probabilistic determinations of certain PIA disclosures causing privacy harm, i.e., if most PC have few links (the long tail) and present comparatively small privacy risk, is regulating its that PIA disclosure an inefficient policy? Perhaps a better social policy would be to attach a lower/no REP. Can we understanding the extent and influence of certain PC on others? How well are certain PC integrated with the whole system, such as data aggregators or online advertising networks?

* How should we apply a scale-free model to privacy controls? For example, does knowing how PC ages (its persistence over time in a network) enhance our understanding of how privacy evolves with time- i.e., does the level of privacy associated with PIA decrease the longer it remains in the network? Can the PC churn rate (the entry and exit of PC within a network) help us understand how quickly PC accumulates links and thus determine the rate of collection/disclosure of PIA? Should the size of PC clusters and their proliferation establish living REP (i.e., our expectations should derive from the flows of PIA), or indicate failure of privacy controls (i.e., the controls that prohibit certain flows are not working)??

* Is there congruence between collection/disclosure topology and the semantic topology of PIA? For example, do the PC cluster based on shared meaning of the value of a particular PIA such as for price discrimination or some other economic application?

6. Operationalizing Scale Free Privacy

Subsequent to validating the aforementioned foundational assumptions, we can operationalize REP to achieve the following intended benefits:

* Inform evidence-based policymaking -- ensure that choice and control of the collection, use and disclosure of PIA is based on empirical reality of how it flows throughout networks; inform default privacy presumptions in an effort to devise more efficient contractual rules, e.g., should we impose implied nondisclosure obligations on certain PC for certain categories PIA? Or, should privacy settings or terms of service establish default REP in web communications?

* Enable better privacy risk management for both individuals asserting privacy rights and entities handling PIA – the entities with countervailing interests—through more predictable outcomes, more certainty about REP determinations, and lower liability risk.

* Advocate common definitional semantics to harmonize reasonable expectations across privacy controls- industry-specific and data-specific laws, geopolitical authorities responsible for enforcing privacy controls, and between and among industries that are largely privacy self-regulated.

* Refute or validate non-institutionalized intuitions about REP norms.

* Devise more sophisticated justifications for our intuitions about privacy (e.g., autonomy, seclusion, property).

* Enhance our understanding of legal and technical controls; improve designs for legal and technical controls; inform standards for triggering privacy controls and for scoping the protection obligation.

Acknowledgements

This research was commenced when author served as Technology Law Advisor at the Center for Applied Internet Data Analysis at UC San Diego. This paper was previously presented at the MIT Data Use Workshop, but not formally published. This research was not advanced beyond what is described herein.

The opinions expressed are those of the author and do not necessarily represent those of the U.S. Department of Homeland Security.