Anticipatory Ethics for a Future Internet:
Analyzing Values During the Design of an Internet Infrastructure

Abstract

The technical details of Internet architecture affect social debates about privacy and autonomy, intellectual property, cybersecurity, and the basic performance and reliability of Internet services. This paper conducts an exercise in anticipatory ethics to understand how a new infrastructure for the Internet might impact these social debates. This paper systematically examines values expressed by an Internet architecture engineering team—the Named Data Networking project—based on data gathered from publications and internal documents. These documents illustrate that networking engineers making technical choices also weigh non-technical values when working on Internet infrastructure. Analysis of the team's documents reveals values invoked in response to technical constraints and possibilities, values that stem from concerns for personal liberties, and values that reflect communitarian leanings. The paper creates a taxonomy of central and peripheral values to demonstrate a method for anticipatory ethics: considering the impact such priorities may have on a future Internet.

1.0 Introduction

> Will we shoot virtually at each other over the Internet? Probably not. On the other hand, there may be wars fought about the Internet. – Vinton Cerf (Fussman, 2008).

The Internet has permeated the economic, political, cultural and social domains of global society and transformed the ways in which individuals, communities, and organizations present and transmit knowledge. The infrastructure underlying the Internet continues to evolve, with ramifications for not only the technical protocols that govern the way the network functions, but also implications for social, economic, and legal issues. Internet protocols affect debates about values such as privacy and autonomy, intellectual property, cybersecurity, and the basic performance and reliability of Internet services. When designing these protocols, engineers must weigh values – abstract interests and goals that become the basis for ethical action (Johnson, 2007; Pinch & Bijker, 1989; Rokeach, 1973). Decades of research in engineering ethics, science and technology studies, and information science have illustrated that values are instantiated in sociotechnical systems. Work practices and cultures can shape values considered during system design (Miller, Friedman, & Jancke, 2007; Shilton, 2013b); these values shape engineers' technical choices (Agre, 1998; Suchman, 1997; Winner, 1980); and some values are in turn concretized in design choices and system rules (Friedman, Kahn, & Borning, 2006; Friedman & Nissenbaum, 1997).

Recent scholarship has suggested that *anticipatory ethics* become a component of the design of emerging technologies (Brey, 2012; Johnson, 2007). Anticipatory ethics is anticipation of how future technologies will be built, how they will be applied, and what their consequences might be. Johnson, in particular, believes that anticipatory ethics should take place quite early in technology development, with the purpose of influencing that development (Johnson, 2011). Practicing anticipatory ethics in tandem with developers may lead to better ethical outcomes and socially responsible technologies.

This paper reports on a project in anticipatory ethics: examining the values considered during the design of a future Internet architecture referred to as Named Data Networking (NDN). The project seeks to understand what values are held by a team of network architects, and how

anticipatory ethics might help us consider the social implications of these values as they are embedded in a new Internet architecture. The Named Data Networking (NDN) project is a high-profile group of network architects working on a fundamental redesign of Internet protocols as part of the National Science Foundation's Future Internet Architecture program. This paper practices anticipatory ethics by asking the following research questions:

1. What values are being considered in the design of NDN?
2. What are the central values espoused by the NDN engineers?
3. How might these values impact design and use of an NDN Internet?

This paper gathers evidence to answer these questions from the NDN team's early publications and internal documents. It traces the salience of particular values to the project, including values central to the project as well as those that are more peripheral (Shilton, Koepfler, & Fleischmann, 2013). Understanding the values espoused by designers in the early stages of design is one method to anticipate the future impacts of this architecture. Values central to the early NDN vision include efficiency and dynamism, as engineers respond to technical constraints and possibilities, as well as values that stem from a concern for personal liberties, including privacy and anonymity. More peripheral communitarian values in the infrastructure include democratization and trust. Understanding the tensions between technical values and social values enables a discussion of how such tensions might influence the future impacts of the NDN architecture. The paper demonstrates an exercise in anticipatory ethics by discussing the implications of these values for information access, public policy, and existing institutional power struggles. By providing an example of how a systematic consideration of design values can contribute to anticipatory ethics, this paper not only illustrates potential impacts of a speculative future Internet architecture; it also advances methods for anticipatory ethics.

2.0 Background

The NDN team at the center of this project was funded by the National Science Foundation (NSF) as part of the NSF's Future Internet Architecture (FIA) program. The NSF has a long history of supporting Internet development (DeNardis, 2009). The FIA program, established in 2010, requested proposals for large projects to develop potential architectures to improve on known problems in the current infrastructure, including security and reliability (National Science Foundation, 2010). The NSF explicitly included values for desirable future Internet architectures in its funding call:

> Proposals submitted must identify architectural requirements that are clearly informed by the legal, ethical and the societal contexts in which the Future Internet will exist. ***Trustworthiness - broadly defined as encompassing security, privacy, reliability, and usability - must be considered as a fundamental design requirement in proposed architectures.*** Other design requirements such as, but not limited to, scalability, openness, ubiquitous access, innovation-enabling, manageability, evolvability and economic viability, may also be considered [emphasis original] (National Science Foundation, 2010).

By evoking legal, ethical and societal contexts, the NSF opened a discussion of values in each of the project teams. Values such as trustworthiness, openness, and economic viability came to be something inscribed in project grant proposals, and shaped purposive features of the architectures themselves. This project investigates this process of concretization and materialization of values in technology on one funded project team: the Named Data Networking project.

2.1 Named Data Networking

The Named Data Networking project was selected as one of four (eventually raised to five) awardees of FIA grants. NDN is a multi-campus research collaboration led by Principle Investigators from the University of California, Los Angeles, and incorporates networking research faculty and students from eight other institutions including University of Arizona; University of California, Irvine; University of California, San Diego; Colorado State University; University of Illinois, Urbana-Champaign; University of Memphis; Washington University; and Northeastern University.

The goal of the NDN team is to research, design and evaluate a replacement for the current foundational layer of the Internet: Internet Protocol (IP). IP relies on addresses to route packets across a global network. Addresses are assigned to hosts across the network by domain registrars, and data is retrieved according to *where* the data is located. NDN changes this equation by making hosting of data irrelevant. Instead, content can be cached anywhere in the network, and is retrieved by the *name* of the data rather than its location in the network (Jacobson et al., 2009).

In more detail, a consumer sends an Interest packet specifying the name of data they wish to receive. The interest packet is forwarded by a series of routers, each seeking a node which has the requested data. Each router remembers only the last interface from which it received the request using a Pending Interest Table (PIT), leaving a single hop-by-hop trail to the data consumer. When the interest packet reaches a router which has the requested data, the router sends a data packet back along this trail, consuming the interest 'breadcrumbs' along the way. Routers can cache copies of the data packet in their memory, creating multiple copies of data to satisfy potential future interests across the web.

The data packet is made up of the name of the data, the content, and a signature verifying the producer of the data using a producer's private key. In this way, NDN also builds security features directly into packets. Each packet must be signed with its producer's public key, thereby verifying its source (Jacobson et al., 2009). This key securely links the name to the data, authenticating that the data is what it purports to be. It ensures that a consumer can trust the data they receive, regardless of the server or router from which it is received. NDN also simplifies public key distribution, because keys can be distributed as content, making cryptography more efficient than for current Internet applications.

With its emphasis on packet provenance, multiple copies and Internet-wide caching, NDN produces many changes for technical aspects of the Internet, from routing to security to application design. These changes in turn will impact social aspects of the Internet, including privacy, law enforcement, governance, and political economy. If we take seriously the notion that code – the technical infrastructures the world relies on every day – shape rights, behavior, and governance (Lessig, 2006), then analyzing how NDN would alter those codes is an important task.

2.2 Anticipatory Ethics

Anticipatory ethics is an emerging practice which seeks to highlight ethical challenges in emerging technology, and use these ideas to shape an ethical conversation during design.

Brey (2012) has suggested a systematic method for conducting anticipatory ethics by analyzing properties of technological objects. Labeled anticipatory technology ethics (ATE), Brey's method focuses on analysis of technological artifacts. Engineers may be consulted to learn about the properties of a technology, but their values are not directly considered.

Johnson (2007) instead advocates direct intervention in design, an approach which is increasingly gaining traction in technology ethics (Fisher, 2007; Shilton, 2013a). She believes it is important for ethics researchers to intervene early in technology development, writing, "the ideas that circulate during the early stages of development of a new technology influence the construction of meaning as well as the material design of the technology" (Johnson, 2011, p. 63). Johnson leaves open, however, the challenge of how best to conduct anticipatory ethics. As she writes, "The hard part is to figure out how to bring ethical notions and practices and ethicists explicitly, intentionally, and effectively into the fray" (Johnson, 2011, p. 67).

This paper contributes to this challenge by providing one method for performing anticipatory ethics: systematic analysis of values in technology design, and exploration of what impacts those values may have. This approach focuses on the agency of designers, using empirical methods to describe what values are considered important by designers in early phases of design. Loo (2012) has suggested that design is a practice of performing ethics. Through the process of design, values are surfaced, exposed, and negotiated. This negotiation in turn affects the shape and characteristics of the resulting technology, and eventually the social impact of design products (Le Dantec, Poole, & Wyche 2009). A values analysis is just one step within anticipatory ethics. Such an analysis can also compliment other forms of anticipatory ethics, such as formal analysis of built features (Brey, 2012), real-time technology assessment (Guston, 2011), or ethics interventions (Fisher, 2007; Manders-Huits & Zimmer, 2009; Shilton, 2013a).

2.3 Values in Network Design

The intersection of information systems and values is an important question facing both social scientists and engineers. The design of technology is never value-neutral, and questions of what, and whose, values are embodied in software and system architecture have been controversial for decades (Alsheikh, Rode, & Lindley, 2011; Friedman, 1997). Affordances built into a technology may privilege some uses (and users) while marginalizing others, highlighting values as a critical if sometimes invisible influence on the design process. Internet network architecture, in particular, carries a number of questions about values in its design. Challenges and social debates like network neutrality (Lemley & Lessig, 2001), wiretapping backdoors (Landau, 2011), and cybersecurity (Clark & Landau, 2011) would all be affected by the implementation of Named Data Networking. These issues are usually examined and addressed after the networks are built and running (Braman, 2012). This project explores values at the point of design, to make explicit social considerations a part of design practice.

To explore the ways in which social values manifest in, and are challenged and changed by network architecture, this work employs a theoretical framework based in *values in design* or *values-sensitive design* (Friedman et al., 2006; Knobel & Bowker, 2011). These traditions explore the ways in which social values become part of technological artifacts. Values are understood to contribute to technology design, to shape system affordances which in turn mediate technology use, and to pervade the social contexts which technology mediates (Kaptelinin & Nardi, 2012; Verbeek, 2006). Values are also personal, shaping how people evaluate their behaviors, respond to others, and make judgments (Rokeach, 1973; Schwartz, 1992). However, the values considered by designers, the values built into design, and the values implications of a designed technology do not always have a predictable, one-to-one correspondence (Albrechtslund, 2007). This paper suggests a first step in a longer process to consider the shift in values implications from design to use. Considering the values salient to designers, and the values intended by designers, can be a first step to understanding what choices

are concretized in design, and suggests potential social impacts of a technology (Shilton et al., 2013).

This paper investigates the values that the NDN team considers central to, and purposive within, their speculative future Internet architecture. The qualifier "salient" implies that individual or collective values will be more important in one situation or context, while other values have more importance in another situation. Intention, a continuum from accidental to purposive values, describes the degree to which a designer or system intends to materialize a value (Shilton et al., 2013). Purposive values are those that are deliberately built into a technology by its designers, and are made material through the technology's affordances and policies.

By describing their early visioning and planning processes, this paper explores what values the NDN team intends to build into the new architecture. Future work will interrogate design decisions as well as the architecture itself to examine whether these purposive values are performed in resulting technological decisions.

3.0 Methods

In the spirit of understanding "the ideas that circulate during the early stages of development" (Johnson, 2011, p. 63), this paper uses published documents from the first year of the NDN project to identify values expressed during the very early design of NDN protocols. We used these documents to understand the central and peripheral values espoused by NDN engineers, and how they might be purposively deployed within the architecture. To address this question, we use a grounded theory approach (Corbin & Strauss, 2007; Lofland, Snow, Anderson, & Lofland, 2006) to analyze values themes within NDN documents and develop a typology for identifying and understanding values in NDN design.

First, the author identified three founding "vision" documents to examine for evidence of values-based rationalizations and justifications for design decisions. These three founding documents are referred to frequently by NDN project team members and subsequent NDN publications. The first document was the original grant application written to fund the project; the second was the "vision" section of the NDN website (http://www.named-data.net/vision.html); and the third was the first academic paper detailing NDN authored by NDN Co-PIs (Jacobson et al., 2009). These documents were written for broad but primarily technical audiences, and were each designed to convince; i.e. they are examples of persuasive writing that contain statements about the foundations, visions and goals of the project. This made the documents excellent places to begin the search for values of importance to the project.

The author and a graduate student assistant performed open coding of these documents independently using the Coding Analysis Toolkit (CAT) software (http://cat.ucsur.pitt.edu). We agreed to use data-driven, inductive codes to identify both semantic (named in the text, such as "privacy") and latent (implied in the text, such as "equity") social values (Braun & Clarke, 2006). We defined values as "significant social goals ascribed to by the authors," and both coders were instructed to assign labels to any statements made about social goals in the text. This resulted in assigning a value term to justifications, ethical debates and conflicts, identification of social quandaries, and stories about actions based on values. We coded each paper at the sentence level. Sentences which did not express semantic or latent social values were not coded.

Once coding of all three documents was complete, the researchers met to discuss values vocabulary, coding differences, and conflicts between codes. We identified disagreements (for example, disentangling "privacy" and "anonymity,") and grouped conceptually similar codes

under a single value. For example, we folded the original code "provenance", which labeled instances of concern with data authorship, into "security." We similarly combined "data minimization," which was only coded once, with the more general term "privacy," which was widely used in all three documents. And we folded "empowerment," coded twice by only one coder, into "equity," which was used by both coders. We resolved coding differences through discussion and consensus. After this code construction process, we were left with thirteen values codes identified across three texts.

The final step was to group these thirteen values into overarching values approaches using theoretical frameworks from the values and design literature. The findings section below discusses these groupings, and the literature from which the groupings were drawn.

4.0 Findings: Purposive Values in the NDN Project

The open coding process produced thirteen final values codes, displayed in the graph below. We tallied the frequency of each code at the sentence level, e.g., how often a written statement expressed a particular value. (Sentences could express more than one value). The frequencies for each value are indicated in Fig. 2. We provide frequencies not as a definitive measure of importance (because factors like the occasional reuse of text between the documents may skew absolute numbers), but instead to provide a qualitative sense for how *central* these values were to founding documents. Frequently-repeated values signify a conceptual importance to the written arguments of the NDN team. This frequency provides a starting point to evaluate the relative salience of these values to design.

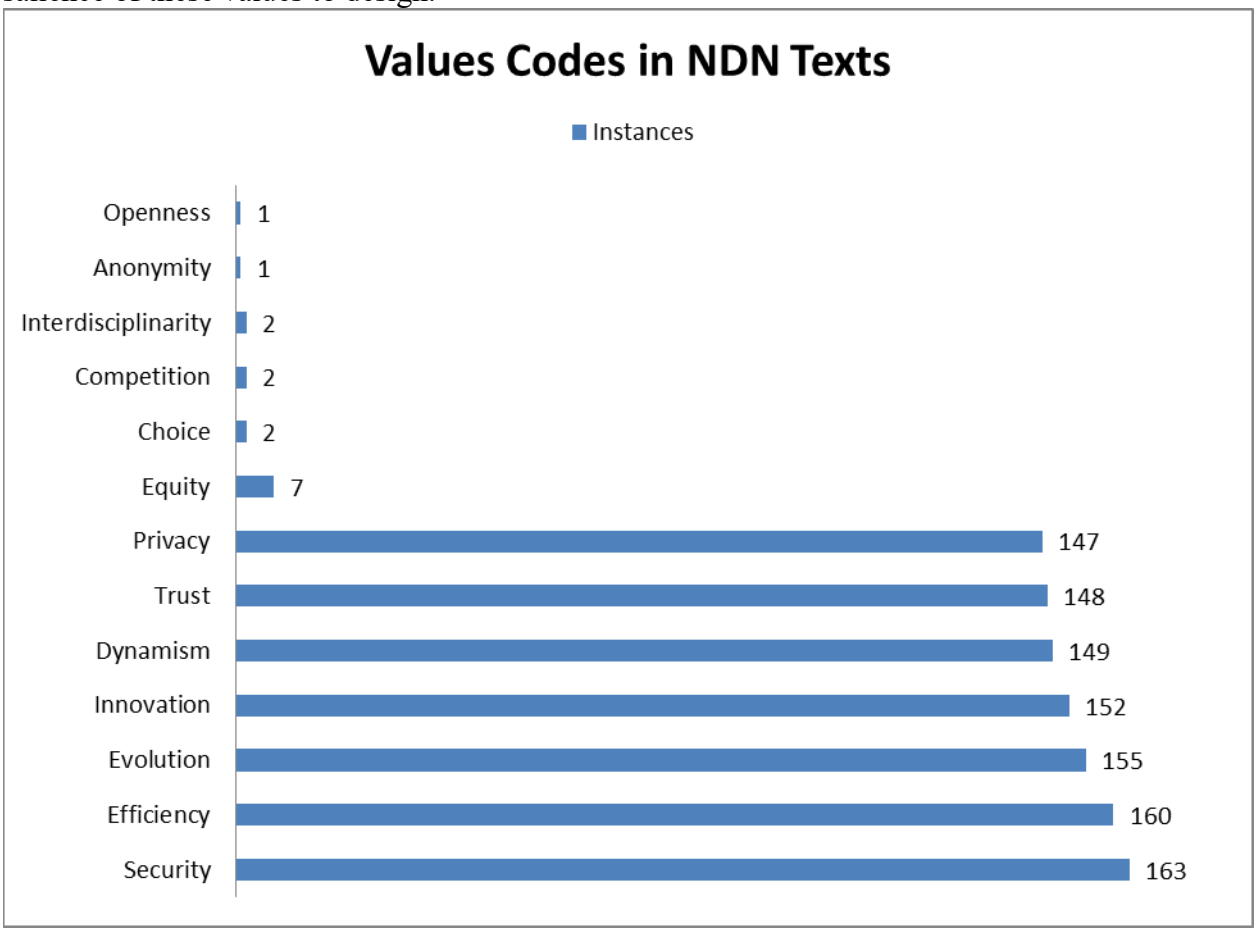

Figure 1: Values codes and frequencies

The frequency of values claims is highly bifurcated; unsurprisingly, values originally mentioned in the FIA call for proposals such as trust, security, privacy, evolvability (evolution) and innovation, dominate the initial NDN documents, including the grant proposal. However, new values also appear: efficiency, dynamism, and a few less frequently-discussed values such as equity, choice, competition, interdisciplinarity, anonymity, and openness.

To better understand what impact such values might have on the NDN architecture, we have grouped these values into theoretical categories suggested by the values in design literature. This develops a taxonomy to understand the different types of values intended in the NDN project. The taxonomy consists of three types of values: 1) those that respond to technical pressures and opportunities; 2) those focused on personal liberties; and 3) those influenced by an interest in the collective concerns of an information commons. A focus on technical pressures is common in the design literature, and has been studied in numerous values and design investigations (Friedman et al., 2006; Friedman & Nissenbaum, 1997). A focus on personal liberties is characteristic of cyber-libertarianism, a standpoint in technology design and use studied by Dahlberg (2010) and Winner (1997), among others. A focus on collective concerns and information commons espouses values found in research and advocacy by popular public intellectuals such as Lessig (2006) and Zittrain (2008).

Technical Pressures	Personal Liberties	Collective Concerns
Dynamism	Evolution	Trust
Efficiency	Privacy	Equity
Innovation	Anonymity	Democratization
Security	Security	

Table 1: Values taxonomy

4.1 Responding to technical pressures

The most frequently-expressed values in the NDN founding documents were those responding to technical pressures. This is not surprising in a research setting where technical innovation is the primary motivator and marker of success. And indeed, many of the values emphasized by the NSF request for proposals were technical values such as scalability and reliability (National Science Foundation, 2010).

Dynamism was expressed most frequently and was often invoked in response to the static nature of IP, which causes problems for data providers using mobile devices. NDN is intended to respond well to the needs of mobile content providers, making the design dynamic. Arguments that illustrated dynamism as a value included statements like, “Even when connectivity is rapidly changing, [NDN] can always exchange data as soon as it is physically possible to do so” (Jacobson et al., 2009, p. 4).

Efficiency was expressed as frequently as dynamism. A primary goal of networking research is building faster networks, and this was reflected in a focus on efficiency in the founding documents. Efficiency was illustrated in comparative statements like, “Content transfer via [NDN] is always secure, yet the results show that it matches the performance of unsecured HTTP and substantially outperforms secure HTTPS” (Jacobson et al., 2009, p. 10).

Innovation was another frequently expressed value. These documents were written by an engineering research team, and it is their primary job to be inventive. Demonstrating innovation to funders and the public is consequently an important goal for the NDN team. Statements like the following illustrate innovation:

> Many future Internet applications will expand the vision of ubiquitous computing to high definition content and interactivity, integrating sensing and control, distributed processing, and user interfaces, at scales and complexity far beyond today's applications. …NDN's intrinsic support for naming data, broadcast, caching, and fine-grained authentication provide obvious advantages to future content-centric application developers (Zhang et al., 2010).

Finally *security*, which is considered a primary weakness of the current Internet's architecture (Clark & Landau, 2011), surfaced as a major technical focus of the NDN architecture and the research team. Security is defined as fortifying the architecture against attacks (such as denial of service or spoofing) from bad actors. All three founding documents emphasize security as a problem with a technical solution. Security in NDN is comprised of two parts – signed packets to verify the provenance of content, and optional encryption to secure individual pieces of content. References to security were often framed like the following:

> At the lowest layers, [NDN] content validation … verifies that content was signed by the key it purports (the key whose fingerprint is specified as the content publisher). …. Even this minimal verification can be surprisingly useful, particularly in defending against many types of network attack (Jacobson et al., 2009, p. 7).

Within these documents, the authors frame security as a technically-inspired value: something required by the technical failings of the current Internet (e.g. the failure of trusted servers or directories to enforce access control). However, security could also be construed as a social value, important to both personal liberties (e.g. to protect personal assets) and collective action (e.g. to protect free speech). Security concerns could be addressed through social or policy means such as removing incentives for bad actors or passing stricter regulations. (For ideas in this vein, see Bauer & van Eeten, 2009). Values like security are boundary-spanning values: values that could be either technically and socially-inspired. Privacy (discussed below) may be another boundary-spanning value. The fact that the NDN engineers frame security as a technical problem to be solved through data validation and encryption, rather than primarily a social challenge, reflects the design context. An FIA project which does not have technical solutions for security problems would not be responsive to the NSF's guidelines, nor the networking community's understandings of the needs of a future Internet. NDN engineers bracket the social side of security as *trust*, a central, collective value discussed below.

4.2 Boosting personal liberties

Perhaps more interesting than the technical values responding to research mandates are a second group of frequently-expressed values, which signaled a concern with personal freedoms and liberties. These values reflected cyber-libertarian underpinnings, a common theoretical and political stance among engineers (Dahlberg, 2010; Winner, 1997). Cyber-libertarianism emphasizes freedom of information and consumer ability to choose over collectivism or regulation (Rey, 2011). As Cohen (2012) describes it, these values support a "rational chooser" who "corresponds to the conventional understanding of negative liberty as the absence of overt constraint" (2012, Chapter 5, p. 5). These values focus on removing constraints on the individual.

The first of these values was *evolution*. Evolution expressed the hope that the NDN architecture could be adopted gradually and purely through market forces, without the need for government intervention. This was in contrast to, for example, IP version 6, which needs

government intervention to succeed – and has been languishing for years (DeNardis, 2009). Statements like the following illustrate evolution:

> Any routing scheme that works well for IP should also work well for [NDN], because [NDN]'s forwarding model is a strict superset of the IP model with fewer restrictions… (Jacobson et al., 2009, p. 5).

Similarly, *privacy* is a value that emphasized personal liberty. Privacy, like security and reliability, was emphasized in the original NSF funding mandate (National Science Foundation, 2010). The NDN architecture responds to privacy concerns with a technical solution: encryption of private data. But importantly, the NDN response emphasizes allowing consumers to decide when encryption is necessary to protect privacy, emphasizing a rational-choice consumer model of information privacy. Examples of statements about included:

> [NDN] does not require trusted servers or directories to enforce access control policies; no matter who stumbles across private content, only authorized users are able to decrypt it (Jacobson et al., 2009, p. 8).

Decisions about when to encrypt are left to content producers in the NDN architecture, demonstrating a privacy model based upon individual choice.

Finally, *anonymity*, while mentioned infrequently on its own, was similar to the value *privacy*. The NDN architecture guarantees anonymity for content consumers such that no one can trace a person's data consumption habits. Consumers of data therefore have a right to privacy regulated by code rather than law. Though it is little-discussed in written documents (largely because it is grouped under the rubric of privacy), the structural importance of anonymity in the NDN architecture reflects cyber-libertarian values of freedom of information seeking and freedom from surveillance and monitoring (Dahlberg, 2010).

4.3 Supporting collective concerns

While personal freedoms are most central to the NDN vision documents, the NDN team's values reflect the influence of information commons and communitarian perspectives. These commons discourses have been pursued by a number of scholars of the Internet (Lessig, 2006), and examples of communitarian values are both central and peripheral to the NDN project.

Trust, for example, was a frequently-discussed value in the foundational NDN literature. NDN engineers discuss trust in data as a quality ensured through provenance information, which rides along with each packet sent over the network. The NDN authors illustrated trust with statements like:

> [NDN] does not mandate a one-size-fits-all trust model. Trust is between publishers and content consumers, and what is appropriate for one application might not be appropriate for another (Jacobson et al., 2009, p. 7).

The NDN documents noted that trust models will need to be social and collectively established by content publishers and consumers to account for this variability.

Much less frequently discussed, but of interest because of its communitarian qualities, were *equity* and *democratization*. Both the grant text and the conference paper briefly discuss the democratization or decentralization of hosting, caching, and information resources enabled by NDN. When it was raised, democratization was discussed as follows:

> NDN democratizes content distribution.... NDN's built-in caching capability enables content producers, be they CNN or a home user, to distribute their content

> at global scale efficiently without special infrastructure such as [content distribution networks], which will have far-reaching impacts on the society, especially for people in underdeveloped regions and in underrepresented groups (Zhang et al., 2010).

Concerns about equity had a similar pattern of discussion focused on equalizing the playing field for content distribution. For example, the website vision statement put it this way:

> This design choice allows any node to freely use all of its connectivity to solicit or distribute data, and removes the information asymmetries that give today's dominant providers disproportionate control over routes and thus over disenfranchises smaller, local providers.

In IP, hosting and caching are centralized and paid for by huge corporations such as Google and Amazon. Content distribution networks (CDNs) such as Akamai will host content close to urban centers for a fee, making this expensive content quicker and easier to access. Both hosting and caching would be decentralized in NDN, happening across many privately-held routers instead of in large data centers. The authors of NDN argue that this model is more democratic for small content producers and producers in the developing world.

5.0 Anticipating the Social Impacts of Design Values

The salience of diverse values in NDN design provide a portrait of the social and technical problems that NDN engineers believe should be addressed through their design. This portrait can be a tool for anticipating ethical concerns now, and shaping future inquiry into ethical considerations of changes to Internet design. This section traces an exercise in anticipatory ethics based on the values explored in early NDN documents, and suggests how typologies like the one developed in this paper can be used for future work in anticipatory ethics.

Analyzing values embraced in the early publications and internal documents of the NDN project allows technology ethics researchers to begin the process of anticipating the social impacts of those design values. Anticipatory ethics is necessarily inexact; some of these impacts will come to be, others will not. But discussing them now can help both ethics researchers and engineers consider whether they embrace the possible social impacts suggested by their architecture.

The values choices embedded in changes to networking proposed by the NDN project may change the ways in which end users experience the Internet through new distributions of resources and power (DeNardis, 2009). NDN would impact several distributions of resources and power, including protection of privacy, access to knowledge, and trust and authenticity of data. It would also have an impact on existing institutional power struggles.

Though NDN's focus on *dynamism* and *efficiency* has technical, rather than ethical, motivations, design choices made to support dynamism and efficiency may impact power arrangements surrounding the existing Internet, therefore evoking ethical concerns. NDN engineers' choice to distribute and cache content broadly over networks would alter current models of how content is delivered. This would impact content delivery networks (CDNs), businesses which currently exist to host content in geographic proximity to consumers. Changes to the market for distribution of data could shake up current market structures, lessening the need for both CDNs as well as centralized hosting services such as YouTube. Encouraging caching across the network is also likely to impact current methods of digital rights management. NDN protocols will encourage the creation of multiple copies of verified content. It will challenge

existing enforcement methods like take-down notices, and perhaps increase the need for technical DRM methods reliant on encryption. NDN's provisions for dynamism and efficiency may also impact developing countries, in particular by infinitely expanding the Internet name space. Domain names are currently limited and efforts to shift to IPv6 have so far been unsuccessful (DeNardis, 2012). Because names are locally determined in NDN, the protocol would eliminate the need to expand the domain name space. Though *equity* concerns were less explicit in early NDN writings, a focus on dynamism and efficiency may eventually impact equity within the global Internet architecture by changing current market structures.

NDN's technical emphasis on *security* will also have social impacts. Consumer-facing impacts might include greater security for applications such as e-commerce and banking, which would be less likely to be spoofed in an NDN Internet. Because content is authenticated in NDN, consumers do not need to worry about the security of either hosts or the pipes over which the data was transmitted. Ensuring that sensitive sites were accessed using SSL protocols, for example, would be unnecessary, because the source of all packets (for example, the bank you trust) would be verified, and sensitive packets (such as financial transactions) would arrive encrypted. So while NDN architects' focus on security is technical in orientation, their implementations of this value may also impact personal liberties such as privacy and consumer rights.

The focus on *privacy*, and the resulting expanded use of cryptography, will likely challenge deep packet inspection and law enforcement. Police and regulatory regimes have long been wary of cryptography, as developers have resisted providing back doors for law enforcement to tap communications. NDN's reliance on cryptography could very well face similar resistance from law enforcement. Encrypted communication packets will make the sort of wiretapping routinely conducted by law enforcement much more difficult. Another concern for network policing is deep packet inspection, used for everything from security concerns to managing traffic flow (Bendrath & Mueller, 2011). Deep packet inspection would be thwarted by encrypted packets in NDN.

Similar to privacy, a focus on *anonymity* in NDN will likely have broad social impacts. Anonymity is a complicated social mechanism. It can help to ensure free speech, evade censorship, and promote civic dialogue (Solove, 2010). It can promote intellectual privacy and discovery, as well (Cohen, 1996; Richards, 2013). It can also be used to evade prosecution for criminal behavior. And scholars worry that there is a strong link between anonymity and mob behavior online, in particular hate crimes (Citron, 2010). NDN's protocols guarantee the anonymity of data consumers. Though interest packets create a trail as they are routed in search of a data packet, the trail is erased as soon as a data packet satisfies the interest. Individuals searching for information cannot have those interests traced back to them, making consumption of content anonymous. Anonymous data retrieval could have a large benefit for privacy, allowing individuals to consume controversial political material or socially-stigmatized content without fear of embarrassment or harm. Anonymity for data producers is more complicated in NDN. Because of an emphasis on provenance and verifiability, it is important that producers be identified in some way. Pseudonymity – associating data with a stable identifier that is not linked to an individual or organization – is one solution for producers of controversial or illegal content. Anyone can produce and sign content under an assumed but consistent name, and there's no reason that data names need to be tied to real identities. But true anonymity for content producers will take more advanced technical measures. NDN engineers are experimenting with Tor-like routing to preserve content producer anonymity (DiBenedetto, Gasti, Tsudik, & Uzun, 2012).

NDN will not solve problems of anonymity in one direction or the other. But it will change the defaults, easing anonymity for consumers of information, while complicating anonymity for producers.

As this discussion illustrates, central concern for technical values can still impact both individual liberties and collectivist concerns on the Internet. Though they may write less about their individual or collectivist leanings, as they team operationalizes technical values, they will impact social concerns as well. Practicing anticipatory ethics through values analysis can help researchers highlight these potential concerns.

6.0 Using the Values Typology

Researchers practicing anticipatory ethics can build on project-specific values typologies such as the one developed here to understand how both central and more peripheral values are materialized and concretized during design. A values typology can be a resource for conducting interviews with designers to further interrogate values in design (Shilton, Koepfler, & Fleischmann, 2014). For example, such interviews would give engineers a chance to challenge the typology and the assumptions made during data analysis. A values typology might also shape the focus of participant-observation and ethnographic interventions into design laboratories (Fisher, 2007). For example, participant-observations might focus on boundary-spanning values such as privacy and security to better untangle the motivations behind these values. The same typology might be used to create socio-technical scenarios to engage with stakeholders and future users to reflect on whether the technology challenges their own values (Kulve & Rip, 2011) and to aid in participatory technology assessment (Guston & Sarewitz, 2002; Guston, 2011).

Analysis of values themes in NDN writings also highlights the critical role that funding organizations can play in impacting at least the initial values expressions of engineering teams. The values discussed in early NDN writings were directly responsive to the NSF request for proposals. This indicates that engaging not only with design teams, but with funding agencies, might be a fruitful path for anticipatory ethics.

In this spirit, the results from this analysis will support a next step for anticipatory ethics: fostering a value-sensitive design process by advocating for explicit values discussion in NDN project meetings. In an ongoing project, we are using participant-observation (Spradley, 1980) to investigate how continuing engineering research on architecture and application areas drive values decisions. Consider for example the value of *information equity* proposed by the original NDN project grant. Engineers wrote that naming data instead of relying upon globally-assigned IP addresses will democratize the process of distributing data across the network. But because it is unclear how naming strategies will be implemented, operationalizing the social value of equity as a system value is conceptually challenging. Operationalizing abstract social values into principles that can be incorporated into the NDN architecture will require creating a working definition of abstract principles such as privacy, anonymity, or equity; and then working together to decide how those definitions will apply to, and be supported by, the NDN architecture.

The values typology can also be used to intervene directly within NDN design. Indeed, theorists of the Internet from Lessig (2006) to DeNardis (2009) might argue that communitarian values should be more central to the team's work. Perhaps equity concerns should be central to design, or at least considered alongside technical and libertarian concerns. Further work as a *values advocate* (Shilton, 2013a) within the NDN team may alter the salience of communitarian values, so that concerns from the Internet theory community become more prominent within

design. To promote discussion around less technical values such as equity and empowerment, we may need to intervene in design practice so these become relevant.

Finally, a limitation of this work is that the values typology was developed and deployed in the context of an academic research project. The project was driven by researchers, supported by grant funding, and not dependent upon commercial success. And the technique required analyzing written "vision" documents, such as grant proposals and publications, which may or may not be available for commercial projects. Very few anticipatory ethics projects to date have investigated ethics in commercial software development. Exploring whether techniques such as the values typology can work within commercial software engineering is a critical next step for anticipatory ethics research.

7.0 Conclusion

Named data networking could change the face of global communication and information sharing. Carefully considering what values are built into the design of this infrastructure will emphasize and enrich the humanistic and democratic nature of this cutting-edge technology. By analyzing what values are important to the NDN engineering team, this paper advances research into the social values that may be embedded into the NDN architecture. It constructs a typology to provide a set of values to inquire about and track through NDN design, as well as a theoretical lens through which to examine the ideologies and standpoints of NDN engineers. This work will facilitate deeper knowledge of the social values behind, and the impacts of, emerging information technologies. And this work suggests a systematic method for analysis of values in early engineering discussions to advance anticipatory ethics, and contribute new techniques for implementing desirable social as well as technical values in the design of emerging technologies.

7.0 Acknowledgements

Many thanks to colleagues Jeff Burke, Jes Koepfler, Amalia Levy, and James Neal for discussions and feedback on drafts of this paper, and especially to James for assistance with data coding. Thanks also to colleagues who attended the 2013 iConference Research Paper Development Roundtable, and in particular Dr. Michael Zimmer, for invaluable feedback on earlier drafts. This work is supported by the National Science Foundation under grant # CNS-1040868.

8.0 References

Agre, P. E. (1998). Beyond the mirror world: Privacy and the representational practices of computing. In *Technology and privacy: The new landscape* (pp. 29–61). Cambridge, MA and London: The MIT Press.

Albrechtslund, A. (2007). Ethics and technology design. *Ethics and Information Technology*, *9*(1), 63–72.

Alsheikh, T., Rode, J. A., & Lindley, S. E. (2011). (Whose) value-sensitive design: a study of long- distance relationships in an Arabic cultural context. In *Proceedings of the ACM 2011 conference on Computer supported cooperative work* (pp. 75–84). New York, NY, USA: ACM. Retrieved from http://doi.acm.org/10.1145/1958824.1958836

Bauer, J. M., & van Eeten, M. J. G. (2009). Cybersecurity: Stakeholder incentives, externalities, and policy options. *Telecommunications Policy*, *33*(10–11), 706–719.

Bendrath, R., & Mueller, M. (2011). The end of the net as we know it? Deep packet inspection and internet governance. *New Media & Society*, *13*(7), 1142–1160.

Braman, S. (2012). Privacy by design: Networked computing, 1969–1979. *New Media & Society*, *14*(5), 798–814.
Braun, V., & Clarke, V. (2006). Using thematic analysis in psychology. *Qualitative Research in Psychology*, *3*(2), 77–101.
Brey, P. A. E. (2012). Anticipating ethical issues in emerging IT. *Ethics and Information Technology*, *14*(4), 305–317.
Citron, D. K. (2010). Civil rights in our information age. In *The offensive internet: privacy, speech, and reputation* (pp. 31–49). Cambridge, MA and London: Harvard University Press.
Clark, D., & Landau, S. (2011). Untangling Attribution. *Harvard National Security Journal*, *2*(2). Retrieved from http://harvardnsj.com/2011/03/untangling-attribution-2/
Cohen, J. E. (1996). A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace. *Connecticut Law Review*, *28*, 981–1039.
Cohen, J. E. (2012). *Configuring the Networked Self: Law, Code, and the Play of Everyday Practice*. New Haven & London: Yale University Press.
Corbin, J., & Strauss, A. (2007). *Basics of Qualitative Research: Techniques and Procedures for Developing Grounded Theory* (3rd ed.). Los Angeles: Sage Publications, Inc.
Dahlberg, L. (2010). Cyber-Libertarianism 2.0: A Discourse Theory/Critical Political Economy Examination. *Cultural Politics: an International Journal*, *6*(3), 331–356.
DeNardis, L. (2009). *Protocol Politics: The Globalization of Internet Governance*. Cambridge, MA and London: The MIT Press.
DeNardis, L. (2012). Hidden levers of internet control. *Information, Communication & Society*, *15*(5), 720–738.
DiBenedetto, S., Gasti, P., Tsudik, G., & Uzun, E. (2012). ANDaNA: Anonymous Named Data Networking Application. In *19th Annual Network & Distributed System Security Symposium*. Presented at the 19th Annual Network & Distributed System Security Symposium, San Diego, CA: Internet Society. Retrieved from http://arxiv.org/abs/1112.2205
Fisher, E. (2007). Ethnographic invention: probing the capacity of laboratory decisions. *NanoEthics*, *1*(2), 155–165.
Friedman, B. (Ed.). (1997). *Human values and the design of computer technology*. Cambridge and New York: Cambridge University Press.
Friedman, B., Kahn, P. H., & Borning, A. (2006). Value sensitive design and information systems. In D. Galletta & P. Zhang (Eds.), *Human-Computer Interaction and Management Information Systems: Applications* (Vol. 6). New York: M.E. Sharpe.
Friedman, B., & Nissenbaum, H. (1997). Bias in computer systems. In B. Friedman (Ed.), *Human values and the design of computer technology* (pp. 21–40). Cambridge and New York: Cambridge University Press.
Fussman, C. (2008, April 24). Vint Cerf Interview - Quotes from the Father of the Internet. *Esquire*.
Guston, D. H. (2011). Participating Despite Questions: Toward a More Confident Participatory Technology Assessment. *Science and Engineering Ethics*, *17*(4), 691–697.
Guston, D. H., & Sarewitz, D. (2002). Real-time technology assessment. *Technology in Society*, *24*(1-2), 93–109.

Jacobson, V., Smetters, D. K., Thornton, J. D., Plass, M. F., Briggs, N. H., & Braynard, R. L. (2009). Networking named content. *Proceedings of the 5th international conference on Emerging networking experiments and technologies*, 1–12.

Johnson, D. G. (2007). Ethics and Technology "in the Making": An Essay on the Challenge of Nanoethics. *NanoEthics*, *1*(1), 21–30.

Johnson, D. G. (2011). Software Agents, Anticipatory Ethics, and Accountability. In G. E. Marchant, B. R. Allenby, & J. R. Herkert (Eds.), *The Growing Gap Between Emerging Technologies and Legal-Ethical Oversight* (pp. 61–76). Springer Netherlands. Retrieved from http://link.springer.com.proxy-um.researchport.umd.edu/chapter/10.1007/978-94-007-1356-7_5

Kaptelinin, V., & Nardi, B. (2012). Affordances in HCI: toward a mediated action perspective. In *Proceedings of the 2012 ACM annual conference on Human Factors in Computing Systems* (pp. 967–976). New York, NY, USA: ACM. doi:10.1145/2208516.2208541

Knobel, C. P., & Bowker, G. C. (2011, July). Values in design. *Communications of the ACM*, *54*(7), 26–28.

Kulve, H. te, & Rip, A. (2011). Constructing Productive Engagement: Pre-engagement Tools for Emerging Technologies. *Science and Engineering Ethics*, *17*(4), 699–714.

Landau, S. (2011). *Surveillance or Security?: The Risks Posed by New Wiretapping Technologies*. Cambridge, MA and London: The MIT Press.

Lemley, M. A., & Lessig, L. (2001). The End of End-to-End: Preserving the Architecture of the Internet in the Broadband Era. *UCLA Law Review*, *48*(4), 925–972.

Lessig, L. (2006). *Code: version 2.0*. New York: Basic Books.

Lofland, J., Snow, D., Anderson, L., & Lofland, L. H. (2006). *Analyzing social settings: a guide to qualitative observation and analysis*. Belmont, CA: Wadsworth/Thomson Learning.

Loo, S. (2012). Design-ing ethics. In E. Felton, O. Zelenko, & S. Vaughan (Eds.), *Design and Ethics: Reflections on Practice* (pp. 10–19). London and New York: Routledge.

Manders-Huits, N., & Zimmer, M. (2009). Values and pragmatic action: the challenges of introducing ethical intelligence in technical and design communities. *International Review of Information Ethics*, *10*, 37–44.

Miller, J. K., Friedman, B., & Jancke, G. (2007). Value tensions in design: the value sensitive design, development, and appropriation of a corporation's groupware system. In *Proceedings of the 2007 international ACM conference on Supporting group work* (pp. 281–290). Sanibel Island, Florida, USA: ACM. Retrieved from http://portal.acm.org/citation.cfm?id=1316624.1316668

National Science Foundation. (2010). Program Solicitation: Future Internet Architectures (FIA). Retrieved February 16, 2013, from http://www.nsf.gov/pubs/2010/nsf10528/nsf10528.htm

Pinch, T. J., & Bijker, W. E. (1989). The social construction of facts and artifacts: or how the sociology of science and the sociology of technology might benefit each other. In *The Social Construction of Technological Systems*. Cambridge, MA and London: The MIT Press.

Rey, P. (2011, November 8). Julian Assange: Cyber-Libertarian or Cyber-Anarchist? *Cyborgology*. Retrieved from http://thesocietypages.org/cyborgology/2011/11/08/julian-assange-cyber-libertarian-or-cyber-anarchist/#more-5260

Richards, N. M. (2013). The Perils of Social Reading. *Georgetown Law Journal*, *101*(3). Retrieved from http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2031307

Rokeach, M. (1973). *The nature of human values*. New York: Free Press.
Schwartz, S. H. (1992). Universals in the content and structure of values: Theory and empirical tests in 20 countries. In M. Zanna (Ed.), *Advances in experimental social psychology* (Vol. 25, pp. 1–65). New York: Academic Press.
Shilton, K. (2013a). This is an intervention: foregrounding and operationalizing ethics during technology design. In K. D. Pimple (Ed.), *Emerging Pervasive Information and Communication Technologies (PICT). Ethical Challenges, Opportunities and Safeguards* (pp. 177–192). London: Springer.
Shilton, K. (2013b). Values levers: building ethics into design. *Science, Technology & Human Values*, *38*(3), 374 – 397.
Shilton, K., Koepfler, J. A., & Fleischmann, K. R. (2013). Charting sociotechnical dimensions of values for design research. *The Information Society*, *29*(5).
Shilton, K., Koepfler, J. A., & Fleischmann, K. R. (2014). How to see values in social computing: methods for studying values dimensions. In *Proceedings of the 17th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW 2014)*. Presented at the 17th ACM Conference on Computer Supported Cooperative Work and Social Computing (CSCW 2014), Baltimore, MD: ACM.
Solove, D. J. (2010). *Understanding Privacy*. Harvard University Press.
Spradley, J. P. (1980). *Participant Observation*. New York: Holt, Rinehart and Winston.
Suchman, L. (1997). Do categories have politics? The language/action perspective reconsidered. In B. Friedman (Ed.), *Human values and the design of computer technology* (pp. 91–105). Cambridge and New York: Cambridge University Press.
Verbeek, P.-P. (2006). Materializing morality. *Science, Technology & Human Values*, *31*(3), 361 –380.
Winner, L. (1980). Do artifacts have politics? *Daedalus*, *109*(1), 121–136.
Winner, L. (1997). Cyberlibertarian myths and the prospects for community. *SIGCAS Comput. Soc.*, *27*(3), 14–19.
Zhang, L., Estrin, D., Burke, J., Jacobson, V., Thornton, J. D., Smetters, D. K., … Yeh, E. (2010). *Named Data Networking (NDN) project* (PARC Technical Report No. NDN-0001). Palo Alto, CA: PARC.
Zittrain, J. (2008). *The Future of the Internet--And How to Stop It*. New Haven & London: Yale University Press.