On economic, societal, and political aspects in ICN

Pouyan Fotouhi Tehrani
Weizenbaum Institute / Fraunhofer FOKUS
pft@acm.org

Jochen H. Schiller
Freie Universität Berlin
jochen.schiller@fu-berlin.de

Thomas C. Schmidt
HAW Hamburg
t.schmidt@haw-hamburg.de

Matthias Wählisch
Freie Universität Berlin
m.waehlisch@fu-berlin.de

ABSTRACT

Information-centric networking (ICN), as an antithesis of host-centric networking, denotes a paradigm shift in communication networks. It introduces names to the network layer and favors delocalized content instead of addresses and hosts. ICN is an attempt to design a network tailored to demands of users who only care about data. The simplicity of this basic premise, however, turns out to be rather deceptive; a pitfall in waiting on the path of ICN to wide-scale deployment. Surely users care about data, but they also care about trust, accountability, private communication, and everything else that the current Internet provides beside mere content. This paper is a first attempt in pinpointing the missing non-technical aspects that are crucial to success of ICN as a viable replacement for the Internet.

CCS CONCEPTS

• **Social and professional topics → Computing / technology policy**; • **Networks →** *Network design principles*;

KEYWORDS

ICN, trust, accountability, privacy, policy

ACM Reference Format:
Pouyan Fotouhi Tehrani, Jochen H. Schiller, Thomas C. Schmidt, and Matthias Wählisch. 2020. On economic, societal, and political aspects in ICN. In *7th ACM Conference on Information-Centric Networking (ICN '20), September 29-October 1, 2020, Virtual Event, Canada.* ACM, New York, NY, USA, 3 pages. https://doi.org/10.1145/3405656.3420229

1 INTRODUCTION

Information-centric networking (ICN) denotes a paradigm shift in networking that aims to address shortcomings of host-based IP networking. The unifying premise of different ICN approaches is that (*i*) Internet's primary use is de facto content distribution [3], and (*ii*) users are only interested in content and barely care about its location within the network [11, 12] (*what* vs *where*). In ICN data is decoupled from its host (more specifically its producer) through independent network-wide labels that cater for content retrieval regardless of its actual location. Respectively, instead of addressing hosts and switching packages among them the network layer directly acts on named data objects. The spatiotemporal decoupling of data from its producer also enables in-network caching, mobility, and multi-homing by design. Proponents of ICN argue that this new paradigm can solve a number of technical and non-technical issues [23] which have been plaguing the IP networking partly due to the dual purpose of IP addresses, *i.e.,* both as host names and interface addresses [18]. All the same, skeptics have also expressed their concern about practical advantages of ICN and raised suspicion about its superiority to existing solutions [8, 19].

In the past decades the idea of information-centric networks has been accompanying the network research community in form of overlay networks, *e.g.,* TRIAD [3], up to ambitious network layer replacements of IP, *e.g.,* Named-data Networking [11] (NDN). Yet, there are still no wide-scale deployments of ICN, let alone any concrete implementation that could replace the Internet as we know it. The reason for this might be the fact that the Internet is not a mere technical construct but a sociotechnical ecosystem that composes an indispensable basis of our economic, social, and political life [9, Chapter 1]. So any radical change to the Internet, however technically reasonable, will face the invisible inertia of Internet's societal, political, and economic forces that have been shaped by and been shaping the Internet landscape since its conception. Although this has not gone unnoticed by ICN researchers, the study of non-technical aspects are generally limited to specific conceptualization and implementation of ICN [5, 13, 20].

In this position paper, we argue that acceptability (if not success) of ICN directly depends on its capability of adaptability and integration within the broader context of the Internet, *i.e.,* into the economic, societal, and political contexts. Based on a generic abstraction of ICN we identify and discuss a number of fundamental enablers that needs to be addressed before any ICN approach can reach wide-spread deployment beyond experimental and research settings.

2 ICN IMPLICATIONS BEYOND NETWORK LAYER

Any ICN approach needs to define at least three name bindings (and respective resolution and authentication methods) to cater for name-based data publication and retrieval:

Name to data: maps a name to actual bits.
Name to owner: maps a name to an authorized producer.
Name to location: maps a name to data address(es).

ICN '20, September 29-October 1, 2020, Virtual Event, Canada
© 2020 Association for Computing Machinery.
ACM ISBN 978-1-4503-8040-9/20/09…$15.00
https://doi.org/10.1145/3405656.3420229

These bindings allow assignment of data with names, allocation of names to respective owner, and name-based publication and retrieval of data over the network. In the following we will focus only on these binding and discuss respective practical implications:

1. Names as commodity. With names at its core, ICN needs to address the issue of namespace management as a perquisite for wide-scale deployment [21]. If we assume that in a future internet ICN names are going to take the role of domain names, we can conclude that they will face similar challenges faced by the DNS ecosystem regarding governance, conflict resolution, and regulation both on national and international levels.

2. Power relations in ICN. In a networked society the most crucial form of power is in the hands of those who shape the network and its goals and those who control the inter-network connections [2]. The paradigm shift of ICN causes a respective shift of power along various dimensions which can be observed in the following in terms of the three aforementioned bindings:

Power over data naming: as data is identified solely by its name, controlling the namespace and name assignment or delegation equals the power over existence of data within the network. Filtering specific content, for example, is as easy as denying it a valid name (comparable to confiscating domain names but with no alternative such as direct IP communication).

Power over name ownership: participation in ICN presupposes ownership of or having the rights to use a subset of global namespace. This raises the question of how the power over a global namespace can justly be divided among related international stakeholder to avoid political complications or conflicts (it took 3 years for North Korea to be awarded with its own .kp TLD [10]).

Power over data retrieval: in contrast to the Internet, where the network is only the *messenger* for IP packets, in ICN the network is also responsible to target data before delivery. This would grant network operators with new power over data discovery and retrieval that can directly impact net neutrality and even enhance censorship capabilities.

3. Information-centric trust. Trust in ICN is generally defined in terms of *trustworthiness as security* (see Nissenbaum [17]). Security alone, however, is not necessarily sufficient to establish trust:

Trustworthy data provision: if a producer is authorized to publish under a name, and the data under that name is bound to the respective producer, *e.g.,* through a digital signature, the name to data binding can be considered as authentic. This requires a notarization service, *e.g.,* PKI, and respective trust model.

Trustworthy namespace management: as part of broader ICN governance, trustworthy namespace management, *i.e.,* allocation to legitimate owners and protection of ownership, requires well-defined policies and trustworthy entities to enforce them.

Trustworthy data discovery and delivery: From the perspective of network operators targeting authentic location of a given name remains an open challenge as consulting a name-to-owner directory and verification of signatures are not feasible for network routers/forwarders.

4. Accountability in ICN. Accountability, as an indicator of responsible practices, comprises taking responsibility and accepting consequences, *i.e.,* punishment and compensation of victims [16].

Accountability in data inquiry and provision: name to data and name to owner bindings cater for data origin, *i.e.,* data producer, authentication as the basis of accountability for data provision. Similarly, as data providers are hold liable for the content they produce, consumers are accountable in what they consume. The data-oriented abstraction of ICN, however, leaves little room for consumer identification. Respectively, maintaining accountability for the new class of malicious activity initiated by consumers, *e.g.,* interest flooding [7, 24], remains an open challenge.

Accountability in namespace and name allocation: A logical consequence of names becoming valuable commodity and in turn subject to regulation and dispute is the growing concern of name misassignment and abuse.

Accountability in data discovery and delivery: As the network maintains routing or forwarding states in order to discover and deliver such content, the question arises if the network as such or respectively network operators can be held responsible for possible *contributory* or *vicarious* copyright infringement just by delivering pirated content for example?

5. Private communication. The very idea of ICN is at odds with private communication both in terms of private as in restricted to a specific group of communicating partners as well as private in terms of secret communication, also referred to as *privacy* in ICN literature [1, 4, 6, 14, 15, 22]. With respect to aforementioned binding, we consider three aspects of private communication as follows:

Private as restricted: The data-oriented communication abstraction of ICN which reduces producers and consumers to second class concepts, and the fact that ICN communication is receiver-controlled (reactive) yet receivers can generally neither be addressed nor identified is the main obstacle to private, *i.e.,* restricted, communication.

Private as covert: The name to owner binding alongside the data-oriented security model of ICN appeals to mapping name to their respective owners and securing them through digital signatures. A signature in turn allows authenticating the producer and caters for non-repudiation. This presumably harmless architectural design, however, poses a non-trivial dilemma: anonymity.

Private as confidential: the Achilles' heel of confidentiality are names themselves, specifically human-meaningful and expressive ones which reveal information about the content being carried over the network.

3 CONCLUSION

In this paper, we briefly discussed the ambitious reconception of networking through ICN and the resulting far-reaching consequences. We focussed on arguments beyond mere technical aspects and considered fundamental economic, societal, and political aspects of a potential ICN-Internet. We have shown that the replacement of IP addresses by names also changes the non-technical landscapes of economic forces, power structures, trust relations, accountability, and private communication. Through this work, we hope to have been able to put the emphasis on the role of non-technical issues for acceptance and deployability of ICN on a global scale.

ACKNOWLEDGMENTS

This work was supported in parts by the German Federal Ministry of Education and Research (BMBF) within the projects *I3* and *Deutsches Internet-Institut* (grant no. *16DII111*).

REFERENCES

[1] Somaya Arianfar, Teemu Koponen, Barath Raghavan, and Scott Shenker. 2011. On preserving privacy in content-oriented networks. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking (ICN ’11)*. ACM Press, New York, NY, USA, 19–24.

[2] Manuel Castells. 2011. A Network Theory of Power. *International Journal of Communication* 5 (2011), 773–787.

[3] David R Cheriton and Mark Gritter. 2000. *TRIAD: A New Next-Generation Internet Architecture.* Technical Report. Distributed Systems Group, Stanford University.

[4] Steven DiBenedetto, Paolo Gasti, Gene Tsudik, and Ersin Uzun. 2011. ANDaNA: Anonymous Named Data Networking Application. *CoRR* abs/1112.2205 (Dec. 2011), 18. arXiv:1112.2205

[5] Dirk Trossen and Alexandros Kostopoulos. 2012. Techno-Economic Aspects of Information-Centric Networking. *Journal of Information Policy* 2 (2012), 26–50.

[6] Nikos Fotiou, Somaya Arianfar, Mikko Särelä, and George C. Polyzos. 2014. A Framework for Privacy Analysis of ICN Architectures. In *Privacy Technologies and Policy*, Bart Preneel and Demosthenes Ikonomou (Eds.). Lecture Notes in Computer Science, Vol. 8450. Springer International Publishing, Cham, Switzerland, 117–132.

[7] Paolo Gasti, Gene Tsudik, Ersin Uzun, and Lixia Zhang. 2013. DoS and DDoS in Named Data Networking. In *2013 22nd International Conference on Computer Communication and Networks (ICCCN)*. IEEE Press, 1–7.

[8] Ali Ghodsi, Scott Shenker, Teemu Koponen, Ankit Singla, Barath Raghavan, and James Wilcox. 2011. Information-centric networking. In *Proceedings of the 10th ACM Workshop on Hot Topics in Networks (HotNets ’11)*. ACM Press, New York, NY, USA, 1–6.

[9] Global Commission on Internet Governance. 2017. *Who Runs the Internet?: The Global Multi-stakeholder Model of Internet Governance*. Technical Report. Centre for International Governance Innovation.

[10] Internet Assigned Numbers Authority. 2007. IANA Report on the Delegation of the .KP Top-Level Domain. https://www.iana.org/reports/2007/kp-report-11sep2007.html [Online; accessed 05-July-2020].

[11] Van Jacobson, Diana K Smetters, James D Thornton, Michael F. Plass, Nicholas H. Briggs, and Rebecca L. Braynard. 2009. Networking named content. In *Proceedings of the 5th international conference on Emerging networking experiments and technologies (CoNEXT ’09)*. ACM Press, New York, NY, USA, 1–12.

[12] Teemu Koponen, Mohit Chawla, Byung-Gon Chun, Andrey Ermolinskiy, Kye Hyun Kim, Scott Shenker, and Ion Stoica. 2007. A data-oriented (and beyond) network architecture. *ACM SIGCOMM Computer Communication Review* 37, 4 (Oct. 2007), 181.

[13] Alexandros Kostopoulos, Ioanna Papafili, Costas Kalogiros, Tapio Levä, Nan Zhang, and Dirk Trossen. 2012. A Tussle Analysis for Information-Centric Networking Architectures. In *The Future Internet*, Federico Álvarez, Frances Cleary, Petros Daras, John Domingue, Alex Galis, Ana Garcia, Anastasius Gavras, Stamatis Karnourskos, Srdjan Krco, Man-Sze Li, Volkmar Lotz, Henning Müller, Elio Salvadori, Anne-Marie Sassen, Hans Schaffers, Burkhard Stiller, Georgios Tselentis, Petra Turkama, and Theodore Zahariadis (Eds.). Lecture Notes in Computer Science, Vol. 7281. Springer Berlin Heidelberg, Berlin, Heidelberg, 6–17.

[14] Tobias Lauinger, Nikolaos Laoutaris, Pablo Rodriguez, Thorsten Strufe, Ernst Biersack, and Engin Kirda. 2012. Privacy risks in named data networking: what is the cost of performance? *ACM SIGCOMM Computer Communication Review* 42, 5 (Sept. 2012), 54–57.

[15] Kebina Manandhar, Ben Adcock, and Xiaojun Cao. 2014. Preserving the Anonymity in MobilityFirst networks. In *2014 23rd International Conference on Computer Communication and Networks (ICCCN)*. IEEE Press, 1–6.

[16] Helen Nissenbaum. 1994. Computing and accountability. *Commun. ACM* 37, 1 (Jan. 1994), 72–80.

[17] H. Nissenbaum. 2001. Securing trust online: Wisdom or oxymoron? *Boston University Law Review* 81, 3 (June 2001), 635–664.

[18] Börje Ohlman. 2015. From ID/locator split to ICN. In *2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC ’12)*. IEEE Press, 256–261.

[19] Diego Perino and Matteo Varvello. 2011. A reality check for content centric networking. In *Proceedings of the ACM SIGCOMM workshop on Information-centric networking (ICN ’11)*. ACM Press, New York, NY, USA, 44–49.

[20] Katie Shilton, Jeffrey A. Burke, KC Claffy, and Lixia Zhang. 2016. Anticipating policy and social implications of named data networking. *Commun. ACM* 59, 12 (Dec. 2016), 92–101.

[21] Pouyan Fotouhi Tehrani, Eric Osterweil, Jochen H. Schiller, Thomas C. Schmidt, and Matthias Wählisch. 2019. The Missing Piece: On Namespace Management in NDN and How DNSSEC Might Help. In *Proceedings of the 6th ACM Conference on Information-Centric Networking (ICN ’19)*. ACM Press, New York, NY, USA, 37–43.

[22] Reza Tourani, Satyajayant Misra, Travis Mick, and Gaurav Panwar. 2018. Security, Privacy, and Access Control in Information-Centric Networking: A Survey. *IEEE Communications Surveys & Tutorials* 20, 1 (2018), 566–600.

[23] Dirk Trossen, Mikko Sarela, and Karen Sollins. 2010. Arguments for an information-centric internetworking architecture. *ACM SIGCOMM Computer Communication Review* 40, 2 (April 2010), 26.

[24] Matthias Wählisch, Thomas C. Schmidt, and Markus Vahlenkamp. 2013. Backscatter from the Data Plane – Threats to Stability and Security in Information-Centric Network Infrastructure. *Computer Networks* 57, 16 (Nov. 2013), 3192–3206.