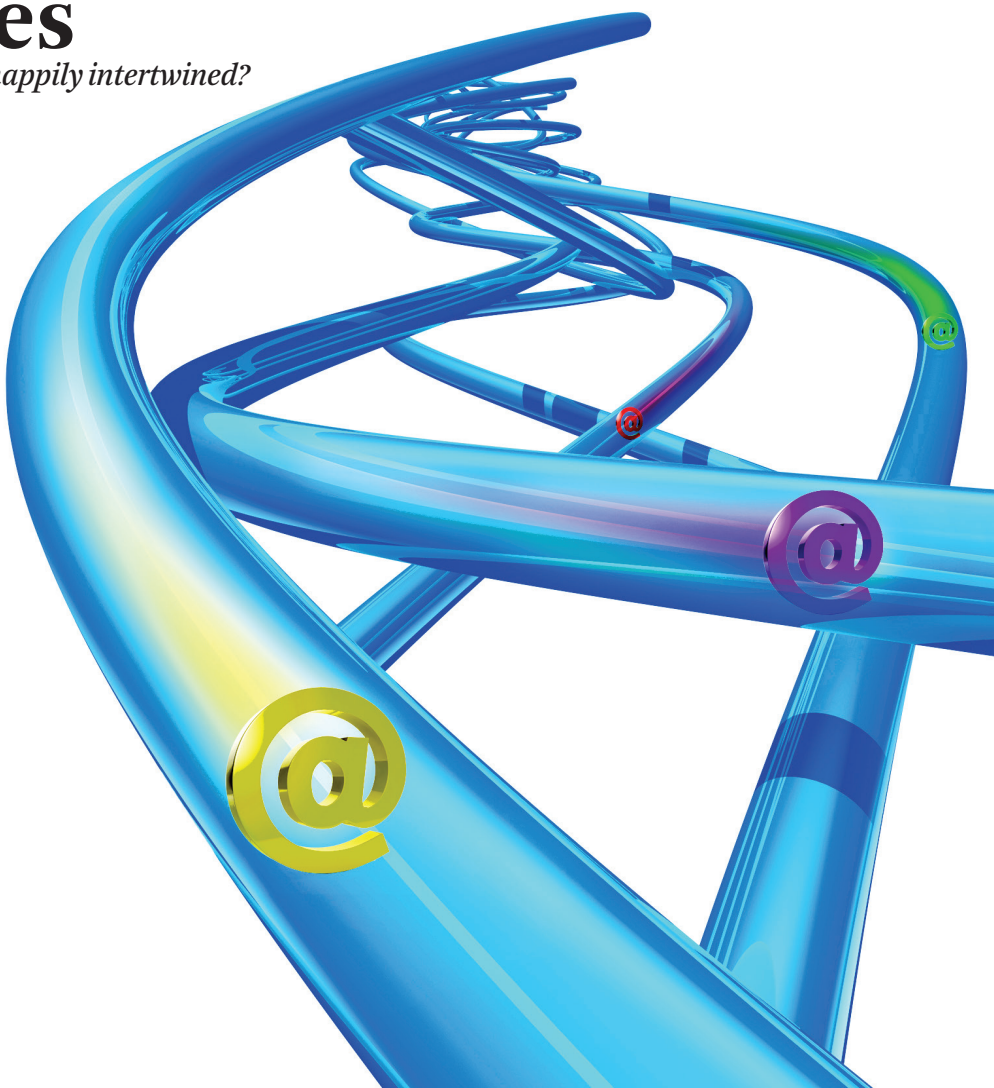
DOI:10.1145/2644146

Stefan Bechtold and Adrian Perrig

Law and Technology
Accountability in Future Internet Architectures

Can technical and legal aspects be happily intertwined?



When the Internet architecture was designed some 40 years ago, its architects focused on the challenges of the time. These included the creation of a distributed communication network that is robust against packet loss and other network failures; support across multiple types of networks and communication services; and the management of Internet resources in a cost-effective and distributed way. As history has shown, the Internet's architects succeeded on many dimensions. The phenomenal success of the Internet has often been attributed to its basic architectural principles.

As the uses of the Internet have expanded beyond the original creators' wildest dreams, its protocols have been stretched to accommodate new usage models, such as mobile, video, real-time, and security-sensitive applications. A string of extensions has resulted in an infrastructure that has increasingly become ossified due to the numerous constraints each extension

introduces, in turn complicating further extensions. These challenges have prompted researchers to rethink architectural principles, thereby engaging in visionary thinking about what a future Internet architecture, which should last for many decades, should look like.

One important dimension of clean-slate Internet architecture proposals is to rethink the role of accountability. The general idea is that accountability for one's actions would enable identification of the offender, making it possible to either defend oneself against misbehavior or deter it altogether. It is therefore natural to consider accountability as a way of addressing network attacks, ranging from route hijacking, to various kinds of network denial-of-service attacks and remote exploitation of host vulnerabilities. Increased accountability could not only address some of the technical shortcomings of the current Internet architecture. It could also enable various partly legal solutions to problems which, to date, have not been solved by purely technical means.

In recent years, security incidents have repeatedly stressed the need for accountability mechanisms. We highlight the use of accountability to address the hijacking of Internet traffic routing by altering or deleting authorized Border Gateway Protocol (BGP) routes. In 2008, YouTube became globally unreachable after a Pakistani Internet service provider (ISP) altered a route in an attempt to block YouTube access in Pakistan. In 2013, the network intelligence firm Renesys documented that traffic routes from Mexico to Washington, D.C., and from Denver to Denver had been rerouted via Belarus and Iceland. In March 2014, Google's Public Domain Name System (DNS) server, which handles approximately 150 billion queries a day, had its IP address hijacked for 22 minutes. During this time, millions of Internet users were redirected to British Telecom's Latin America division in Venezuela and Brazil. Such rerouting, whether deliberate or not, abuses the implicit trust enshrined in the BGP routing protocol. Traffic rerouting is often difficult to detect for both Internet users and network operators. It can be used for a wide range of attacks. Despite the introduction of BGPSEC (a security protocol that promises to stop hijacking attacks), accountability—which makes it possible for an attacker to be identified, sued, and prosecuted—may prove a better solution to the hijacking problem.

Another example where accountability matters is the network neutrality debate. Insufficient accountability mechanisms in today's Internet prevent consumers from finding out why their access to particular services has been blocked or slowed down. Is today's access to Hulu slow due to technical problems at Hulu's servers, due to delays somewhere in the network, or due to bandwidth limitations between your ISP and your home network? It is difficult to determine. More generally, if a technical architecture does not provide means for users to monitor whether service providers keep their promises with regard to service quality and features, service providers may have insufficient incentives to actually keep their promises.

An architecture that leaves loopholes in legal and technical accountability has it costs. As the Internet traffic hijacking example shows, it may encourage unlawful online activities, with all the negative effects this entails for society. As the network neutrality example demonstrates, it may deter business partners from entering into contractual agreements, as their terms may be unenforceable.

Currently, manifold attempts are being made to deal with accountability loopholes. On the legal front, legislators and government agencies are designing rules to provide network providers and users with the right incentives despite limited accountability. In the ongoing battle over network neutrality regulations, for example, the U.S. Federal Communications Commission (FCC) has proposed rules that will force ISPs to disclose their network management practices.[a] In June 2014, the FCC announced it would investigate the impact peering agreements between ISPs such as Comcast and Verizon and content providers such as Netflix have on broadband consumption and Internet congestion.

Security incidents have repeatedly stressed the need for accountability mechanisms.

On the technical front, any technology aimed at increasing accountability should provide irrefutable proof that parties have performed certain actions: in particular, of who is being held accountable for what action to whom. End users, hosts, ISPs (or their routers and network equipment), service operators, or content providers could all potentially be held accountable or be enabled to verify the accountability. Consider a system that would hold an ISP's routers accountable for delayed packet forwarding. It would have to ensure the routers cannot hide the fact they delayed forwarding a packet. Such accountability for delays could serve as a technical measure to validate the network neutrality of an ISP.

Researchers have proposed numerous technical solutions for various types of accountability. Bender et al. propose to hold the source accountable for packets created, and enable each router to verify.[2] Such packet origin accountability is a popular property, which subsequent researchers have pursued with varying assumptions and approaches for cryptographic key setup.[1,3,7] Li et al. propose a general key setup mechanism between sources and network routers to enable packet origin, router forwarding, and routing message accountability.[6] Naous et al. propose a system for packet origin and strong router forwarding accountability.[9] Zhou et al.[11] propose a strong notion of making the network accountable for any state it may have ("secure network provenance"). The same authors have extended their work to also provide time-aware provenance.[12]

a This aspect of the proposed Open Internet Rules has not been affected by the January 2014 decision of the U.S. Court of Appeals for the District of Columbia, which struck down anti-blocking and anti-discrimination obligations.

Implementing only legal or technical measures to increase accountability on the Internet has limitations. We believe it is a fruitful exercise to combine technical and legal aspects for two reasons. First, this challenges perceptions lawyers have about technology and vice versa. As the Internet traffic hijacking and the network neutrality examples demonstrate, it is often difficult to identify what caused network errors. From a legal perspective, lacking identifiability makes it impossible to hold someone accountable for the error. This, in turn, reduces everyone's incentive to prevent network errors, as the risk of being held liable is low. All too often, the legal debate simply assumes such accountability loopholes are a given fact on the Internet. The debate has not considered how liability regimes and the types of contracts and services offered on the Internet would change if a future Internet architecture were to provide enhanced accountability mechanisms. The current lack of accountability, for example, prevents service level agreements that span beyond a single autonomous system. Accountability for network operations could enable an ISP to provide inter-ISP service-level agreements, as the ISP could restrict his liability to internal errors, thereby excluding external errors that can be attributed to the appropriate responsible party. Increasing accountability could thus make liability risks manageable and contractable.

Second, by combining technical and legal aspects of accountability in network design, we can focus on trade-offs in network design decisions that might otherwise pass unnoticed. An important issue is the trade-off between accountability and privacy. Usually they are in conflict, as accountability requires sacrificing privacy.[5] However, in some cases, both can be achieved. For example, Mallios et al. have proposed a system where privacy is achieved as long as a user does not misbehave, whereas misbehavior will render the user accountable.[8,b] Another important trade-off exists between accountability and personal freedom. Lessig argues that e-commerce will require accountability at the cost of personal freedom.[5] There might be other issues here. If everyone's actions on the Internet were traceable, how could political activists communicate under oppressive political systems? How could highly privacy-sensitive citizens communicate? Technical solutions such as anonymous communication systems implemented as an overlay network on the Internet can achieve anonymous communication despite a traceable or accountable underlying network architecture. The important research question is how the two properties can be meaningfully combined. The answer may be something similar to the privacy example described previously: As long as users communicate within some defined traffic pattern, their communications remain anonymous. If they deviate from the pattern, their (potential mis-) behavior can be traced back. It is also worth noting that increased accountability can be advantageous to political activists. In societies where governments control Internet traffic within the country and across borders, increased accountability can impede unobtrusive censorship, as the increase in transparency makes it more difficult for the government to hide its censoring activities.

Many design decisions have implications for social interactions that lie in the realm of the law.

We cannot offer any easy ways to deal with such trade-offs. We can, however, observe that many important problems in today's Internet are due to a lack of accountability and transparency. The response—to increase accountability—is not a mere technical enterprise. Many design decisions have implications for social interactions that lie in the realm of the law. Because law and technology are sometimes interchangeable and sometimes lead to difficult trade-offs, legal considerations should be taken into account not only after a novel Internet architecture has been implemented, but as an integral part of the design process of the architecture itself.[4,10] Such an approach could do more than enhance the value of the architecture itself. Increased accountability may also produce novel services that we cannot envision at present, precisely because of accountability loopholes that affect the current Internet.

As the interaction between network usage and the law increases, the network's technical architecture must cope with trade-offs and policy values that have long been familiar within the legal system. It is one of the challenges of future Internet architecture design to develop holistic approaches that will integrate technical and legal aspects and enable researchers and developers to be versatile in both fields. C

b This works like the detection of double spending in digital cash: a payment is untraceable as long as the user spends the coin only once, but the identity is revealed if the coin is spent twice.

References

1. Andersen, D.G. et al. Accountable Internet Protocol (AIP). In *Proceedings of ACM SIGCOMM*, 2008.
2. Bender, A. et al. Accountability as a service. In *Proceedings of USENIX SRUTI*, 2007.
3. Andersen, D., Parno, B., and Perrig, A. SNAPP: Stateless network-authenticated path pinning. In *Proceedings of AsiaCCS*, March 2008.
4. Flanagan, M., Howe, D.C., and Nissenbaum, H. *Embodying Values in Technology: Theory and Practice.* Cambridge University Press, Cambridge, 2008, 322–353.
5. Lessig, L. *Code and Other Laws of Cyberspace.* Basic Books, NY, 1999.
6. Li, A., Liu, X., and Yang, X. Bootstrapping accountability in the Internet we have. In *Proceedings of USENIX NSDI*, 2011.
7. Liu, X. et al. Passport: Secure and adoptable source authentication. In *Proceedings of USENIX NSDI*, 2008.
8. Mallios, Y. et al. Persona: Network layer anonymity and accountability for next generation Internet. In IFIP TC 11 International Information Security Conference, May 2009.
9. Naous, J. et al. Verifying and enforcing network paths with ICING. In *Proceedings of ACM CoNEXT*, 2011.
10. Nissenbaum, H. How computer systems embody values. *IEEE Computer 34*, 3 (2001), 118–120.
11. Zhou, W. et al. Secure network provenance. In *Proceedings of the ACM Symposium on Operating Systems Principles (SOSP)*, October 2011.
12. Zhou, W. et al. Distributed time-aware provenance. In *Proceedings of the International Conference on Very Large Databases (VLDB)*, August 2013.

Stefan Bechtold (sbechtold@ethz.ch) is Professor of Intellectual Property at ETH Zurich and a *Communications* Viewpoints section board member.

Adrian Perrig (adrian.perrig@inf.ethz.ch) is Professor of Computer Science at ETH Zurich.

The authors would like to thank Srdjan Capkun, Susanne Hambrusch, John L. King, and Timothy Roscoe for helpful feedback.