Faculty of Art

2014

# End user privacy and policy-based networking

Paterson, Nancy

JOURNAL OF INFORMATION POLICY 4 (2014): 28-43.

# END USER PRIVACY AND POLICY-BASED NETWORKING

BY NANCY E. PATERSON*

Are privacy concerns over end user surveillance by network operators such as AT&T and Verizon, and by "edge providers" such as Google and Amazon, being dangerously overshadowed by the predominant emphasis on government surveillance? Quite possibly so, Professor Paterson concludes, after reviewing currently-used packet analysis technologies and their advertised capabilities. Paterson concludes that the problem faced by privacy and public interest advocates is that no one has a truly comprehensive grasp of how widely network operators have deployed such tools, what information is collected, or how it is put to use. Paterson asserts that the potential risks call for additional vigorous research in this area.

## INTRODUCTION

Since the summer of 2013 there has been much attention on Internet surveillance by government agencies. In contrast, this article examines policy-based measures applied to end users through traffic control protocols and practices used by wireline and especially wireless networks. This article suggests that this borders on, or constitutes, surveillance by networks and edge providers. Examples include AT&T, Verizon, and Bell Canada as well as content delivery networks (CDNs) such as Google, Facebook, and Amazon. All of these engage in various types of policy-based networking, creating "tunnels" for forwarding and routing according to each end user's Internet data, in order to define policies in a way that goes beyond the traditional routing protocol practices of the past.

## POLICY-BASED NETWORKING QUALITY OF SERVICE (QOS)

When you tap the touch screen of a mobile smart phone or tablet, typically the desire is for information regarding (for example) banking, friends, or a movie synopsis and geo-location of the movie theatre along with directions for how to get there. How do networks and content companies provide this information? They track you. Despite the influence of raised awareness regarding Edward Snowden and his revelations about the National Security Agency, end users seem to understand little about how the tracking works. They are rarely consulted nor are they informed of

* Associate Professor, OCAD University. The author would like to thank the editors of the Journal of Information Policy and the participants at the "Theory of Broadband: Regulation, Networks and Applications" Experts' Workshop held at Columbia University Center for Tele-Information in June 2013. The author also acknowledges the generous hospitality of Dr. Andrew Clement and the Information Policy Research Program at the Faculty of Information, University of Toronto for providing an ideal environment in which to revise this article.

what is happening with their data and that there may be implications for privacy, either intended or unintended. At the application level most end users freely give up their data and do not mind having their metadata tracked and used, yet some end users seek elusive opt-out privacy options at the application level. Are end users making decisions with full information and have they been given the proper information with which to make that decision? And if the commercial actors have not provided information fully, is that a conscious business decision or did they just neglect to consider it?

Policy-based networking (which could also be considered rules-based networking) is the management of data traffic in a network so that various kinds of traffic –data, voice, and video – are assigned a precedence or type of service (ToS) value in the IP packet headers and endpoints in the network. There are numerous methods for data traffic management to prioritize and control data traffic including deep packet inspection, queuing mechanisms, and load-sharing capabilities. These differentiated traffic practices are often employed for ordinary technical network management, but when differentiated traffic practices are applied to end users, the practice is broadly termed quality of service (QoS). Recommendation E.800 from the International Telecommunication Union formally defines QoS as the collective effect of service performance which determines the degree of satisfaction of a user of the service. Previous definitions present QoS as an attempt to satisfy the user's demands with a service that fulfills the user's needs.[1]

QoS traffic controls such as IP precedence, type of service (ToS), DiffServ, tagging, and packet inspection all evolved over the historical development of the Internet and increasingly enabled differential treatment of each end user's data routing. Deep packet inspection (DPI) covers a range of activities: metering for customer billing, setting data traffic types, control priority for time-sensitive data such as video, and surveillance for security or commercial use. The exact scope and nature of packet inspection usage is not widely agreed upon in the networking community. Here is how one authority, *Heavy Reading*, spells out the parameters for its usage of the term:

> [A] classical definition [of deep packet inspection] would focus on the ability to analyze and understand what a data packet contains, and to what application or service it belongs. This means having visibility up to Layer 7, with the ability to see into the header and payload. However, DPI equipment vendors commonly employ other types of analysis, such as flow-based traffic analysis or behavioral traffic analysis, in conjunction with DPI. We use the term DPI broadly to cover all techniques commonly used to determine, at the greatest possible granularity, what a

[1] International Telecommunication Union, "Definition of Terms Related to Quality of Service," Recommendation ITU-T E.800, Sept. 2008, accessed Feb. 16, 2014, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-E&type=items. See also Sabina Baraković and Jasmina Baraković, "Traffic Performances Improvement Using DiffServ and MPLS Networks," *Proceedings of the ICAT 2009 XXII Information, Communication and Automation Technologies* (Oct. 2009), accessed Feb. 16, 2014, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5348439, 1.

> packet is, to what service or application it belongs, which subscriber sent it, and what type of data the packet contains.[2]

Because bandwidth capacity keeps increasing, most network operators maintain that at present they use packet inspection only for testing and monitoring bandwidth or traffic flows, rather than for examining packets. Yet press releases, specifications, and white papers published by many network analytics and packet inspection equipment manufacturers suggest that deep packet inspection is used to inspect Internet data packets and determine their type and contents so that different types of data traffic can be classified for traffic control purposes. For example, according to network analytics vendor Tellabs, DPI can provide information on user content and context, the application being used, where that user is located at that time, and the class of service to be delivered, as per fee and contract.[3] Other vendors generally confirm that the purpose of deep packet inspection is to identify types of traffic applications being employed by end users (subscriber, device, location) and to associate the metadata gleaned at a refined level.[4] Allot Technologies, Arbor, Procera, Cisco, JDS Uniphase, Sandvine, and Bluecoat all produce deep packet inspection equipment for networks. Allot says this about its NetEnforcer product:

> [D]edicated QoS devices such as the NetEnforcer are based on DPI, which enables them to look much deeper into packets and accurately identify both protocols and applications using the protocols. This enables the efficient classification of and marking of WAN-bound traffic. Seamlessly integrating in multiprotocol label switching (MPLS) networks, such devices can classify and prioritize all traffic before it reaches the access router or carrier edge router, which simply forward traffic.[5]

Bluecoat's PacketShaper DPI equipment has extensive classification abilities to identify and classify applications, then assign appropriate QoS tags.[6] DPI usage is further detailed in a corporate white paper from network analytics company Tellabs. In that perspective, the network uses hardware-based DPI functionality to detect and classify traffic flows, while the access and router platforms together function as the QoS engine:

> Using a scripting language, the [network] operator can program the core platform and select appropriate QoS markings. […] The operator can define rules for

---

[2] Graham Finnie, "Policy Management & DPI Market Tracker," white paper, *Heavy Reading* (2012), accessed Feb. 16, 2014, http://www.heavyreading.com/details.asp?sku_id=2457&skuitem_itemid=1212&promo_code=&aff_code=&next_url=%2Flist.asp%3Fpage_type%3Dall_trackers.

[3] Tellabs, "How the Smart Mobile Internet Transforms Your Business," white paper, June 2011, accessed Feb. 16, 2014, http://info.tellabs.com/rs/tellabs/images/tlab_smartmobleinternet_wp_742360.pdf?mkt_tok=3RkMMJWWfF9wsRonuq/MZKXonjHpfsX96+4pWLHr08Yy0EZ5VunJEUWy2YIGSdQhcOuuEwcWGog81AlUFuGXbw==.

[4] Graham Finnie, "The Role of DPI in an SDN World," white paper, *Heavy Reading*, Dec. 2012, accessed Feb. 16, 2014, http://cdn.sdncentral.com/wp-content/uploads/2012/12/Qosmos_DPI-SDN-WP_Dec-2012.pdf.

[5] Allot Communications, "MPLS and NetEnforcer Synergy: Enhancing the Control of MPLS-Based, Enterprise Managed Services with Allot's NetEnforcer," white paper (2007), accessed Feb. 16, 2014, http://www.ipnetworks-inc.com/pdfs/allot/Allot%20NetEnforcer%20in%20MPLS%20Networks.pdf.

[6] Blue Coat Systems, "Enhance MPLS QoS," accessed Feb. 16, 2014, https://bto.bluecoat.com/packetguide/current/solutions/app-control/enhance-mpls-qos.htm.

> identifying application types, group those types into classes of service and assign traffic-management and QoS actions. Once the core platform detects an application type, usually by inspecting the first few packets on each flow, the operator can assign traffic-management actions at line rate to flows.[7]

## MULTIPROTOCOL LABEL SWITCHING (MPLS) CLASS OF SERVICE, SOFTWARE-DEFINED NETWORKING (SDN), AND MOBILE IPV6

Internet protocol (IP) networks were initially built on the notion of autonomous system networking (ASN). When an end user made a request to view a website, the host name (for example http://www.website.com) was resolved to an IP number by a domain name server (DNS) physically located in the upstream network path. The IP address for the website – and the network that owned or was responsible for hosting the website – was associated with the network's five-digit ASN. The website request would be routed in a series of border gateway protocol (BGP) routing hops via interconnecting ASNs until the website network was reached and the website was retrieved back to the end user. Whether digital subscriber line (DSL), wireless (cellular), or cable (data over cable service interface specification - DOCSIS[8]), edge access technologies were typically used in conjunction with various classic best efforts forwarding and routing protocols.[9]

Intelligent networks today, however, are completely different as they utilize policy-based networking tools such as multiprotocol label switching (MPLS), software-defined networking (SDN), and mobile IPv6 (encapsulated in IPv4). With both MPLS and later SDN, virtualized networking and routing tools operate independently from physical network topology. Unlike traditional IP forwarding, virtualization separates the data forwarding from the control plane and uses protocols to communicate between them. This works by inserting an additional layer of forwarding information (in the form of a label or tag) that allows the operator to control the flow of traffic on the network, allowing the end user's applications to "tunnel" as if they had the entire network to themselves, despite the fact that they are sharing it.[10]

MPLS and SDN ostensibly invite comparisons as they both deal with routing technologies and practices, but IPv6 seems a dissimilar technology to include in this discussion. It is included because it provides advanced routing efficiency and end user data traffic control in comparison to the efficiencies that were offered first by MPLS and later by SDN. IPv6 as applied in mobile networks provides for the explosive growth of 4G users and the resulting increased demand for Internet Protocol (IP) addresses. Mobile IPv6 allows mobile device users to move from one network to

---

[7] Tellabs, 5.
[8] "DOCSIS" stands for Data Over Cable Service Interface Specification.
[9] Jonathan S. Nuechterlein and Philip J. Weiser, *Digital Crossroads: American Telecommunications Policy in the Internet Age* (Cambridge, MA: MIT Press, 2005), 32, 124.
[10] Graham Finnie, "Policy Control and SDN," white paper, *Heavy Reading*, Aug. 2013, accessed Feb. 23, 2014, https://www.sandvine.com/solutions/cost-reduction/sandvine-and-heavy-reading-policy-control-and-sdn-a-perfect-match.html, 7, 9.

another while maintaining a permanent IP address, and it supports seamless and continuous Internet connectivity for data including VoIP. Mobile IP specifies how a mobile user registers with their network and how the network routes the data through a specified "tunnel" for that user.[11] Because the "tunneling" is a concept in all three technologies, this article uses the term *policy-based networking* for the protocols that increasingly utilize this tunneling.

### *Multiprotocol Label Switching (MPLS) Class of Service*

Multiprotocol Label Switching (MPLS) is an older part of the growing area of policy-based forwarding, and thus numerous arguments have been developed regarding its role in the scheme of complex classification technologies. Examining its usage is instructive in exploring the emergence of the software-defined networking that came later. While MPLS was originally employed for its tunneling capability, it gradually became more widely employed for its traffic control capabilities. MPLS allows "numerous diverse networks to operate as a single, integrated network."[12] Unlike routing at each border router in a data traffic path, MPLS allows the initial router to determine the route and label to be embedded in the packet routing instructions, as shown in Figure 1 below. Routers in the network's core simply execute those instructions, reducing normal packet processing time.[13]

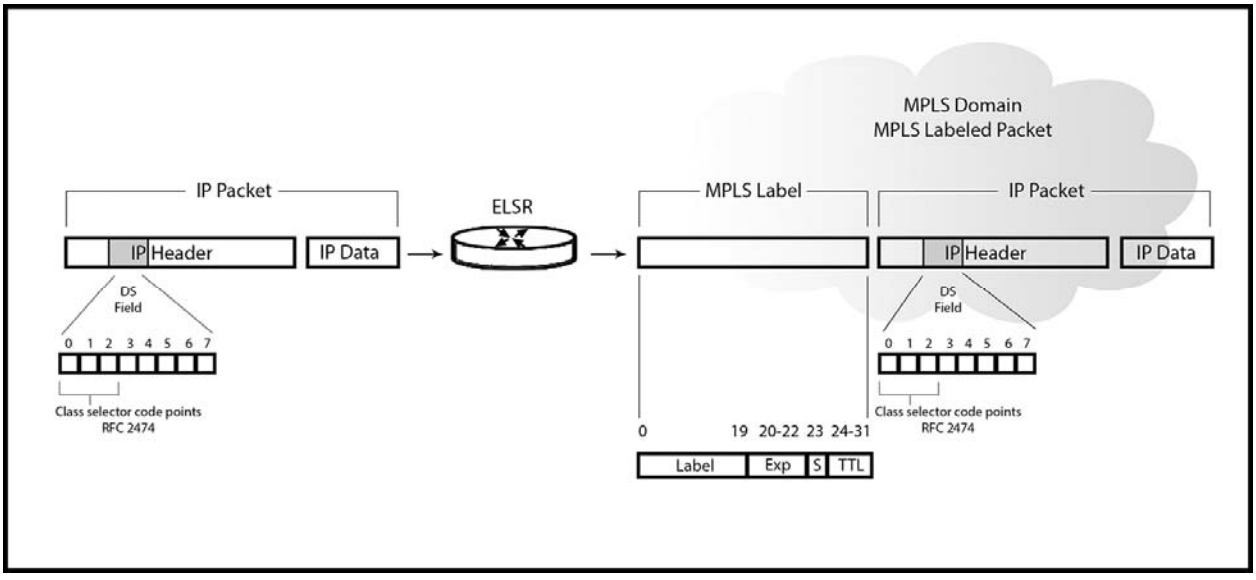


*Figure 1: IP packets ingress to MPLS through an edge label switching router.*

[11] Patrick Hubbard, "With SDN, IPv6 Transition May Not Be So Hard," *Techtarget*, Nov. 2013, accessed Feb. 23, 2014, http://searchsdn.techtarget.com/opinion/With-SDN-IPv6-transition-may-not-be-so-hard; Kaushik Das, "What is Mobile IPv6?" IPv6.com, accessed Feb. 23, 2014, http://ipv6.com/articles/mobile/Mobile-IPv6.htm.
[12] Andrew Dolganow and John Fischer, "Application-Aware MPLS Tunnel Selection," United States Patent No. 20090213858 A1, Aug, 27, 2009, accessed Feb. 16, 2014, http://www.google.com/patents/US20090213858.
[13] David Greenfield, "Europe's Virtual Conundrum," *Network Magazine* 15, no. 11 (Nov. 2000): 119. See also John William Evans and Clarence Filsfils, *Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice* (San Francisco: Morgan Kaufmann, 2007).

In a continuation of QoS traffic management practices such as IP precedence, ToS, and tagging, MPLS classification often consists of rewritten tags attached to data packets, to which MPLS adds its own labeling. MPLS is not the technology for Internet traffic inspection or analysis in specifying class of service; as discussed previously, packet inspection equipment is used for this purpose. As noted by William Stallings in his textbook *Data and Computer Communications*, traffic policy parameters for Internet packets are specified by networks, and the first requirement of data classification is outside the scope of MPLS: "[T]he assignment needs to be done either by manual configuration, or by means of some signaling protocol, or by an analysis of incoming packets at ingress LSRs [MPLS routers]."[14]

### *Software-Defined Networking (SDN)*

Partly because MPLS capabilities are vendor-proprietary, in late 2012 SDN emerged as an alternative policy-based networking technology, often incorporating a tool or tools similar to OpenFlow. OpenFlow features software-based (as opposed to hardware-based) dynamic routing and vendor interoperablility.[15] One challenge in understanding these emerging technologies is that there is no universally agreed-upon definition of what is meant by software-defined networking. In the past, most definitions have hinged on the decoupling of the network control plane from the network forwarding plane, a concept already familiar from MPLS. Some current definitions of SDN focus less on decoupling and more on the provision of programmatic interfaces in network equipment, as opposed to whether or not there is a separation of the control and forwarding planes. Most proposals to apply SDN to policy forwarding make use of the tags and label swapping of the MPLS forwarding plane (amongst other types of forwarding in hardware) and either ditch the MPLS control plane or reduce it a dumb helper.[16]

OpenFlow is the result of research collaboration between Stanford University and the University of California at Berkeley, and is backed by Verizon, NTT, and others.[17] The Open Networking Foundation (ONF) has developed the OpenFlow specification for the enterprise market. What remains unclear, however, is whether this specification will be widely embraced for carrier deployments of SDN; OpenFlow is only one way to do SDN. In its more radical variants, SDN brings revolutionary change to network architectures. A separate initiative emerged in October 2012, led by a group of twelve major network operators including AT&T, BT, Deutsche Telekom, Orange, Telefónica and Verizon, under the rubric of "Network Functions Virtualization." The group called for "international collaboration to accelerate development and deployment of

[14] William Stallings, *Data and Computer Communications*, 9th Ed. (Upper Saddle River, NJ: Prentice Hall, 2010), 676.
[15] Steve Wallace, Uwe Dahlmann, Ron Milford, and Chris Small, "Openflow in a Day," presentation at NANOG58, New Orleans, LA, June 3, 2013, accessed Feb. 23, 2014, http://www.nanog.org/sites/default/files/mon.tutorial.wallace.openflow.31.pdf.
[16] Marc Mendonca, Bruno Astuto A. Nunes, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti, "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," May 24, 2013, under review at *IEEE Communications Surveys and Tutorials*, accessed Feb. 23, 2014, http://hal.inria.fr/docs/00/82/50/87/PDF/SDN_survey.pdf, 11, 13, 14.
[17] Jim Duffy, "FAQ: What is OpenFlow and Why Is It Needed?" *Network World*, Apr. 14, 2011, accessed Feb. 16, 2014, http://www.networkworld.com/news/2011/041411-open-flow-faq.html.

[virtualized network functions] based on industry-standard servers."[18] Despite these marketplace uncertainties and the fact that much of the detail in SDN remains to be resolved, it appears that SDN deployments will continue to expand.

What makes policy-based forwarding via SDN and packet inspection unique is that the rules for classification are more highly determined than the simple destination IP, source IP, and ToS bits. The potentially unsettling aspect of these new developments in policy-based forwarding is the capability to pick off fine-grained traffic flows and degrade or even hijack traffic, with a high degree of invisibility and therefore minimal transparency. The ability of deep packet inspection to identify data traffic types and traffic classification means this technology can identify end user metadata at increasingly granular levels, which may raise privacy concerns:

> [The] SDN plan strongly suggests that one vital requirement will be the collection, analysis and presentation, as a usable resource, of detailed intelligence from the network – a function for which DPI is well suited, and already playing a vital role in the majority of networks today. Core current concepts such as load balancing, Layer 4-7 switches, policy management and application delivery controllers (ADCs) – which rely on a deep, real-time insight into higher layers that identifies applications and other metadata on traffic – are likely to play an even bigger role in an SDN network than they do today.[19]

Networks rely on packet labeling to improve traffic engineering and routing performance, by stipulating an explicit path in routing for each end user. Packets are given special labels to denote what type they are (VoIP, e-mail, video, peer to peer, gaming, etc.).[20] Business customers typically predetermine their classifications before sending upstream to networks, whereas for consumer end users, classification is defined by the Internet Service Provider. Privacy concerns may arise from the fact that the end user IP numbers, type of device, geographic location, and type of data traffic or application, as well as content, can all be aggregated together in a relatively non-transparent process.

### *Mobile IPv6*

The provisioning of LTE 4G cellular networks to manage the many types of data traffic generated by the thousands of apps and other services used by customers requires development of further traffic management practices. As shown in Figure 2 below, Mobile IPv6 is the use of encapsulated IPv6 in IPv4 routing, providing QoS for new applications such as IP telephony, video/audio, interactive games, or e-commerce. This technology allows a smart phone, tablet, or computer to remain reachable regardless of its location in an IPv6 network and ensures that transport layer connections survive. With the help of Mobile IPv6, even though the mobile node changes locations and addresses, the existing connections through which the mobile node is communicating are

[18] Finnie, "The Role of DPI in an SDN World," 5.
[19] Ibid., 7.
[20] Christian Esteve, Fabio L. Verdi, and Mauricio F. Magalhaes, "Towards a New Generation of Information-Oriented Internetworking Architectures," *Proceedings of the 2008 ACM CoNEXT Conference*, Article No. 65 (2008), accessed Feb. 16, 2014, http://www.cs.ucla.edu/classes/cs217/2008TowardsANewGenerationOfInformation-Oriented.pdf.

maintained. To accomplish this, connections to mobile nodes are made with a specific address that is always assigned to the mobile node, and through which the mobile node is always reachable. IPv6 addresses the main problem of IPv4: that is, the exhaustion of addresses to connect computers or hosts in a packet-switched network. IPv6 has a very large address space and consists of 128 bits as compared to 32 bits in IPv4. IPv6 enables the transformation that occurs at the networking infrastructure level. It also provides resources and functions to make software-defined networking (SDN) and network virtualization scale more easily. IPv6 facilitates and simplifies virtualization across the entire infrastructure, including network, computing, and storage resources.[21]

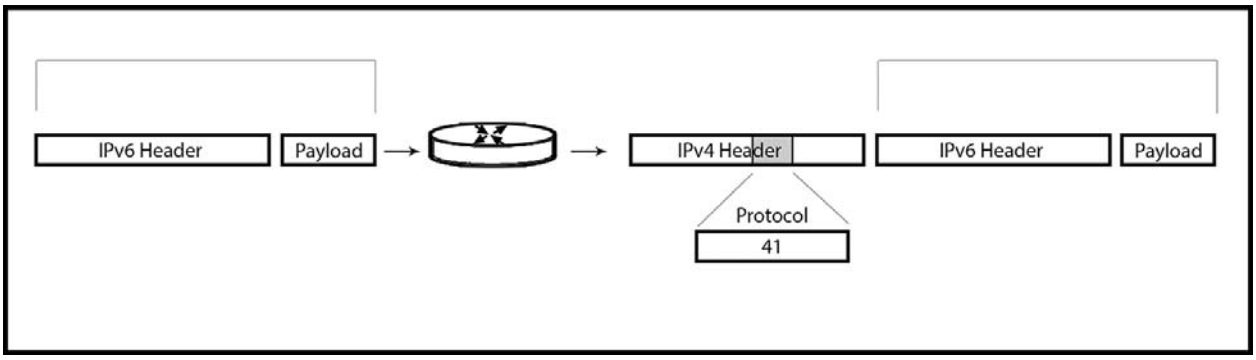


*Figure 2: IPv6 packets tunneled inside IPv4.*

Cellular communications operating from a single cell tower are part of a local sub-network. The connection between the cell tower and the public Internet begins with a backhaul link to the core of the network. In wireless networks, end users have multiple devices (laptops, cell phones, desk phones, tablets) connecting to multiple networks (LTE 4G, 3G, WiFi), all relying on unique authentication methods and different QoS and tunneling protocols. Radio access networks (RAN) are exponentially more complex than the wireline and core network. Mobile service providers are migrating their networks to all-IP to be capable of delivering real-time, bandwidth-intensive services like video. In the past, MPLS was deployed by many mobile service providers to consolidate disparate transport networks (CDMA, GSM, LTE) for different radio technologies. This infrastructure supports mobile evolution to Long Term Evolution (LTE), Worldwide Interoperability for Microwave Access (WiMAX), Fourth-Generation Mobile Network (4G) technologies, and full fixed-mobile convergence (FMC).[22] In current practice, MPLS is increasingly

[21] Hubbard.
[22] Alcatel-Lucent, "Deploying IP/MPLS in Mobile Networks," white paper (2010), accessed Feb. 16, 2014, http://www3.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=White_Papers/CPG2896100928_Deploying_IPMPLS_in_Mobile_Networks_EN_StraWhitePaper.pdf, 3.

being replaced by a combination of mobile IPv6 and newer software-defined networking (SDN) in cell site gateways for the commensurate "fine grained measurement and control" of metadata.[23]

In its latest stage of development, the 4G LTE platform promises 4 Gb/second of download speed and GPS technology for mobile devices, providing the ability to pinpoint the end user's exact location and type of Internet activity. It also incorporates multiple application utilization, such as simultaneous use of voice and data. End users typically pay service providers for one or more application-specific service level agreements. According to a 2009 Alcatel-Lucent patent, each end user "pays a first amount for a guaranteed level of service with respect to a first application, while paying a different amount for a guaranteed level of service with respect to a second application."[24]

At present, LTE technology is being deployed and is more fragmented than the previous third-generation wireless technology. Analysts quoted by the Wall Street Journal estimate that there are 36 LTE bands around the world, compared with 22 bands for the most popular version of 3G technology:

> LTE […] only works with networks operated by Verizon Wireless and AT&T in the U.S., and Bell Canada, Rogers Communications Inc. and Telus Corporation in Canada. IDC data shows that only three countries in the world have significant numbers of LTE customers: the U.S., South Korea and Japan. Verizon currently has the largest LTE network in the world and the highest number of LTE subscribers.[25]

## END-USER PRIVACY AND POLICY-BASED NETWORKING

In Canada, the tendency of new networking protocols to prompt privacy concerns can be found in official Canadian assessments of privacy in the "cloud computing" arena. At the federal level, in October 2013 the Privacy Commissioner of Canada launched an investigation when Bell Canada released information regarding end user tracking and collection of network usage information to serve up relevant ads to its mobile customers. The Public Interest Advocacy Centre and the Consumers' Association of Canada filed a subsequent application with the Canadian Radio-television and Telecommunications Commission complaining that Bell Canada's actions violated telecom policy. The two groups argue that the tracking runs counter to Canadians' reasonable expectations of privacy and say that the company's privacy policy is actually insufficient to protect people's privacy. The groups stated that Bell is "overstepping its role as a neutral provider of

[23] Li Erran Li, Z. Morley Mao, and Jennifer Rexford, "Cell SDN: Software-Defined Cellular Networks," white paper, Bell Labs (2012), accessed Feb. 16, 2014, http://www.bell-labs.com/user/erranlli/publications/CellSDN-TR12.pdf, 1.
[24] Dolganow and Fischer.
[25] Jessica E. Vascellaro, Sam Schechner, and Spencer E. Ante, "New iPhone to Support LTE," *Wall Street Journal*, Sept. 7, 2012, accessed Feb. 16, 2014, http://online.wsj.com/news/articles/SB10000872396390443819404577637903902952754.

telecommunications services" and is also "double-dipping" in that the company is charging customers for a service and then using the information collected for marketing purposes.[26]

In the United States, privacy issues have been addressed in proposals published by the Federal Trade Commission (FTC). In February 2012, the FTC issued a report called *Protecting Consumer Privacy in an Era of Rapid Change,* which recommended that Congress consider enacting general privacy legislation, data security and breach notification legislation, and data broker legislation.[27] A year later, in February 2013, the FTC took up the issue of mobile networks, issuing a list of recommendations as to how application developers could do a better job of protecting end user privacy by offering much clearer statements concerning the information they collect across mobile networks.[28]

It is difficult to ascertain at this juncture just how secure or insecure end user data or metadata may be as it traverses public networks. Analysts at the Surveillance Studies Centre at Queen's University in Canada have investigated cross-border information issues, with particular attention to the sharing of airline passenger information between the United States government and American companies. Sharing issues include "the relative lack of accountability within US data-handling organizations, the out-sourcing to private companies of data transferred south to the US, and the exemptions that many state and private organizations involved in US Homeland Security enjoy from US privacy law."[29] Currently, no single authority regulates preferential (positive or negative) class forwarding in either the United States or Canada. Additionally, some carriers argue that because consumers have many options open to them for telecommunications services, they should no longer be regulated as utilities. AT&T and other carriers, including Verizon, have persuaded many states to repeal regulations, alleging that they are outdated in an era when people have a host of alternative ways to communicate. In the fall of 2012, AT&T CEO Randall Stephenson said that the carrier would try to repeal landline regulations at the state level.[30]

Do carrier and edge networks guard end user data or metadata when utilizing policy-based virtual networking? Until fairly recently the answer would have been yes. However new products like Verizon's Precision Market Insights, unveiled in late 2012, show otherwise. The product offers businesses like shopping malls, stadiums, and billboard owners statistics about the activities and backgrounds of cellphone users in particular locations. Several European mobile network operators

---

[26] Christine Dobby, "Public Interest Groups File CRTC Complaint over BCE's Customer Tracking Policy," *Financial Post*, Jan. 27, 2014, accessed Feb. 16, 2014, http://business.financialpost.com/2014/01/27/public-interest-groups-file-crtc-complaint-over-bces-customer-tracking-policy/?__lsa=64a3-e389.

[27] Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change*, report, Mar. 2012, accessed Feb. 16, 2014, http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

[28] Ina Fried, "Feds Urge App Makers, Mobile Operating Systems to Do Better on Privacy," *All Things D*, Feb. 1, 2013, accessed Feb. 16, 2014, http://allthingsd.com/20130201/feds-urge-app-makers-mobile-operating-systems-to-do-better-on-mobile-privacy/.

[29] Alanur Çavlin Bozbeyoğlu, "The Private Sector, National Security and Personal Data: An Exploratory Assessment of Private Sector Involvement in Airport and Border Security in Canada," report to the Office of the Privacy Commissioner of Canada, Surveillance Studies Centre, Mar. 2011, accessed Feb. 16, 2014, http://www.sscqueens.org/sites/default/files/OPC_Final_31_March.pdf, 6.

[30] Anton Troianovski, "AT&T Move Signals End of the Copper-Wire Era," *Wall Street Journal*, Nov. 7, 2012, accessed Feb. 16, 2014, http://online.wsj.com/news/articles/SB10001424127887324439804578104820999974556.

have launched similar efforts. German software giant SAP AG has introduced a service that will gather smartphone usage and location data from wireless carriers and offer it to marketing firms.[31]

Similar questions are being asked about Internet publishers and content delivery networks such as Facebook, Yahoo!, Google, and Amazon, which have made huge investments in network infrastructure in order to meet the daunting challenges of network routing and storage scalability required to service their millions of customers. These firms employ custom networking hardware and software-defined networking with large-scale parallel processing algorithms and associated datasets across their entire computing pool.[32] For example, Facebook brings in 500 TB of new data per day and uses the Hadoop distributed file system, an open source version of Google's proprietary GFS system, for storing and retrieving large datasets.[33] In April 2013, Facebook officially launched a new tool to help advertisers gather information from Facebook users based on their offline spending history. The tool marries what Facebook already knows about each user's friends and "likes" with vast troves of information from third-party data marketers such as Datalogix, Acxiom, and Alliance Data Systems. These firms collect data from the webpages consumers visit, the e-mail lists on which they have signed up, and their online and offline spending patterns.[34]

According to Jordan Robertson of Bloomberg, there are dozens of networks that collect and share details from apps and connect marketers to users with tailored ads. AdMob (owned by Google) and Millennial Media are the two biggest aggregators for Android, the largest smartphone operating system in the world.[35] And documents released by former National Security Agency contractor Edward Snowden to the *New York Times*, the *Guardian*, and *ProPublica* show that the United States and United Kingdom have infiltrated mobile software for details about users' movements and social affiliations. Among the apps with the greatest privacy perils are Google Plus, Pinterest online bulletin boards, and Candy Crush Saga (the most popular game on Facebook).[36]

All these developments will continue to expand the market for intelligent routing, along with the associated forms of technologies and controls described in this article, which have replaced the traditional model of autonomous, mutually assistive networking:

> [T]here is no doubt that Layers 4-7 will become a critical focus for the future. Indeed, if SDN is successful, the nuts and bolts of networking will fade into the background, and the needs of applications and subscribers will move into the foreground. On this reading, network service providers will gradually morph into

[31] Anton Troianovski, "Phone Firms Sell Data on Customers," *Wall Street Journal*, May 21, 2013, accessed Feb. 16, 2014, http://online.wsj.com/article/SB10001424127887323463704578497153556847658.html.
[32] Open Networking Foundation, "Software-Defined Networking: The New Norm for Networks," white paper, Apr. 13, 2012, accessed Feb. 16, 2014, https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf.
[33] Dave Shine, "Intro to Hadoop," speech before the Orlando.net User Group, Apr. 18, 2013.
[34] Evelyn M. Rusli, "Buy Signal: Facebook Widens Data Targeting," *Wall Street Journal*, Apr. 9, 2013, accessed Feb. 16, 2014, http://online.wsj.com/news/articles/SB10001424127887324504704578412960951909032.
[35] Jordan Robertson, "Google+, Candy Crush Show Risk of Leakiest Apps," *Bloomberg*, Jan. 29, 2014, accessed Feb. 16, 2014, http://www.bloomberg.com/news/2014-01-29/nsa-spying-on-apps-shows-perils-of-google-candy-crush-.html.
[36] Ibid.

> applications service providers – with all that this implies. DPI [deep packet inspection] and related techniques will be at the heart of that transformation. It will create a virtuous circle or feedback loop in which a stream of real-time information on performance, application use trends, user behavior, congestion events, device trends and much else besides is fed back to the SDN controller and to the various network and consumer applications connected to it. Using policy and related tools (e.g. optimization software), this will allow for continual adjustment to circumstance, optimizing both the efficiency with which resources are consumed and the quality of the end-user experience.[37]

The application of new technologies for end user traffic control and classification in virtual routing and networking may be considered another form of invasion and surveillance. Citing a recent text by security specialist Bruce Schneier entitled "Liars and Outliers: Enabling the Trust that Society Needs to Thrive," Somini Sengupta of the *New York Times* says "[T]he liars he worries about most are not cyberwarriors or even cybercriminals but private companies and government agencies advancing their own interests, whether for surveillance or commerce."[38]

## CONCLUSION: THE ECONOMICS OF PRIVACY

Privacy is a vague concept with a lot of theoretical explorations. Can classic notions of privacy as physical, such as not tolerating someone snooping around your home or personal possessions, be extended into modern matters of "virtual" privacy and control over end user information? At the application level, most end users freely give up their personal data and do not mind having their metadata tracked and used. Yet some end users seek opt-out privacy options at the application level and find these options elusive. Both types of end users experience deep packet inspection and traffic controls at lower levels of the network to gather and use metadata. Use of end user metadata is not regulated, meaning that there are no checks in place to guard against the eventuality that some network operators might expand their application of these technologies.

To take an example, P2P traffic can be readily inspected and discarded through the use of classification and differentiated services. In contrast, gaming networks receive specialized treatment. In the future, the simple combination of social networking with air travel bookings and payments could be a compelling candidate for the creation of a novel class of service. Yet this type of combination may be considered suspect. "Conspirator analysis" is a term from Internet law, similar to "aiding and abetting" in criminal law. If both the network and whoever buys the end user data or metadata have conspired to set up systems in ways that make personal data trackable, then they could be considered as engaged in a conspiracy to violate user privacy. In the future, efforts to

[37] Finnie, "The Role of DPI in an SDN World," 10.
[38] Somini Sengupta, "Trust: Ill-Advised in a Digital Age," *New York Times*, Aug. 11, 2012, accessed Feb. 16, 2014, http://www.nytimes.com/2012/08/12/sunday-review/bruce-schneier-an-avatar-of-digital-distrust.html.

provide end users with security for their e-commerce transactions and similar applications may indicate the need for new forms of protection for end user privacy.

"The economics of privacy" is a relatively new theoretical area for online communications, in which the users of personal data claim that the economic benefits of traffic controls, surveillance, targeted ads, etc. can trump traditional privacy concerns.[39] If someone owns information and someone else wants to buy it, this is a legitimate business transaction. Additionally, even if end user metadata did come to enjoy new forms of privacy protection, such protection would likely be applied on an *ex post* rather than *ex ante* basis, thus requiring considerable initiative on the part of untrained end users to recognize and report inappropriate or unsanctioned uses of their metadata. It gets more political if we consider the wishes of the end users that the information is about, and whether the sellers and buyers of that information have structured the system to reduce requirements for end users to enter data. Lastly, user input could be commercialized; for example, in the future privacy-seeking end users might have a model like Pay-TV in which the end user pays more for service that has no metadata collection.

The problem faced by privacy and public interest advocates today is that no one has a truly comprehensive grasp of how widely network operators have deployed policy-based networking tools, nor the extent to which end user information is being aggregated by these tools and put to uses that may create risks for the privacy and security of the end users. The dilemma here, as with so much else in the online privacy debate, is that millions of end users, like those who use Facebook, see the benefits of policy-based networking tools without being aware of the potential risks. In any case, it now seems indisputable that the deployment of policy-based network infrastructure, combined with metadata intelligence, calls for continuing, vigorous research into all the technological and social aspects of this emerging topic.

[39] Alessandro Acquisti, "The Economic Theory of Personal Data and Privacy," Background Paper No. 3 (Dec. 1, 2010), Joint WPISP-WPIE Roundtable, accessed Feb. 23, 2014, http://www.oecd.org/sti/ieconomy/46968784.pdf.

## BIBLIOGRAPHY

Acquisti, Alessandro. "The Economic Theory of Personal Data and Privacy." Background Paper No. 3 (Dec. 1, 2010), Joint WPISP-WPIE Roundtable. Accessed Feb. 23, 2014, http://www.oecd.org/sti/ieconomy/46968784.pdf.

Alcatel-Lucent. "Deploying IP/MPLS in Mobile Networks." White paper (2010). Accessed Feb. 16, 2014, http://www3.alcatel-lucent.com/wps/DocumentStreamerServlet?LMSG_CABINET=Docs_and_Resource_Ctr&LMSG_CONTENT_FILE=White_Papers/CPG2896100928_Deploying_IPMPLS_in_Mobile_Networks_EN_StraWhitePaper.pdf.

Allot Communications. "MPLS and NetEnforcer Synergy: Enhancing the Control of MPLS-Based, Enterprise Managed Services with Allot's NetEnforcer." White paper (2007). Accessed Feb. 16, 2014, http://www.ipnetworks-inc.com/pdfs/allot/Allot%20NetEnforcer%20in%20MPLS%20Networks.pdf.

Baraković, Sabina and Jasmina Baraković. "Traffic Performances Improvement Using DiffServ and MPLS Networks." *Proceedings of the ICAT 2009 XXII Information, Communication and Automation Technologies* (Oct. 2009). Accessed Feb. 16, 2014, http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5348439.

Blue Coat Systems. "Enhance MPLS QoS." Accessed Feb. 16, 2014, https://bto.bluecoat.com/packetguide/current/solutions/app-control/enhance-mpls-qos.htm.

Bozbeyoğlu, Alanur Çavlin. "The Private Sector, National Security and Personal Data: An Exploratory Assessment of Private Sector Involvement in Airport and Border Security in Canada." Report to the Office of the Privacy Commissioner of Canada, Surveillance Studies Centre, Mar. 2011. Accessed Feb. 16, 2014, http://www.sscqueens.org/sites/default/files/OPC_Final_31_March.pdf.

Das, Kaushik. "What is Mobile IPv6?" IPv6.com. Accessed Feb. 23, 2014, http://ipv6.com/articles/mobile/Mobile-IPv6.htm.

Dobby, Christine. "Public Interest Groups File CRTC Complaint over BCE's Customer Tracking Policy." *Financial Post*, Jan. 27, 2014. Accessed Feb. 16, 2014, http://business.financialpost.com/2014/01/27/public-interest-groups-file-crtc-complaint-over-bces-customer-tracking-policy/?__lsa=64a3-e389.

Dolganow, Andrew and John Fischer. "Application-Aware MPLS Tunnel Selection." United States Patent No. 20090213858 A1, Aug, 27, 2009. Accessed Feb. 16, 2014, http://www.google.com/patents/US20090213858.

Duffy, Jim. "FAQ: What is OpenFlow and Why Is It Needed?" *Network World*, Apr. 14, 2011. Accessed Feb. 16, 2014, http://www.networkworld.com/news/2011/041411-open-flow-faq.html.

Esteve, Christian, Fabio L. Verdi, and Maurıcio F. Magalhaes. "Towards a New Generation of Information-Oriented Internetworking Architectures." *Proceedings of the 2008 ACM CoNEXT Conference*, Article No. 65 (2008). Accessed Feb. 16, 2014, http://www.cs.ucla.edu/classes/cs217/2008TowardsANewGenerationOfInformation-Oriented.pdf.

Evans, John William and Clarence Filsfils. *Deploying IP and MPLS QoS for Multiservice Networks: Theory & Practice*. San Francisco: Morgan Kaufmann, 2007.

Federal Trade Commission [United States]. *Protecting Consumer Privacy in an Era of Rapid Change*. Report, Mar. 2012. Accessed Feb. 16, 2014,

http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

Finnie, Graham. "Policy Control and SDN." White paper, *Heavy Reading*, Aug. 2013. Accessed Feb. 23, 2014, https://www.sandvine.com/solutions/cost-reduction/sandvine-and-heavy-reading-policy-control-and-sdn-a-perfect-match.html.

———. "Policy Management & DPI Market Tracker." White paper, *Heavy Reading* (2012). Accessed Feb. 16, 2014, http://www.heavyreading.com/details.asp?sku_id=2457&skuitem_itemid=1212&promo_code=&aff_code=&next_url=%2Flist.asp%3Fpage_type%3Dall_trackers.

———. "The Role of DPI in an SDN World." White paper, *Heavy Reading*, Dec. 2012. Accessed Feb. 16, 2014, http://cdn.sdncentral.com/wp-content/uploads/2012/12/Qosmos_DPI-SDN-WP_Dec-2012.pdf.

Fried, Ina. "Feds Urge App Makers, Mobile Operating Systems to Do Better on Privacy." *All Things D*, Feb. 1, 2013. Accessed Feb. 16, 2014, http://allthingsd.com/20130201/feds-urge-app-makers-mobile-operating-systems-to-do-better-on-mobile-privacy/.

Greenfield, David. "Europe's Virtual Conundrum." *Network Magazine* 15, no. 11 (Nov. 2000): 116-123.

Hubbard, Patrick. "With SDN, IPv6 Transition May Not Be So Hard." *Techtarget*, Nov. 2013. Accessed Feb. 23, 2014, http://searchsdn.techtarget.com/opinion/With-SDN-IPv6-transition-may-not-be-so-hard.

International Telecommunication Union. "Definition of Terms Related to Quality of Service." Recommendation ITU-T E.800, Sept. 2008. Accessed Feb. 16, 2014, https://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.800-200809-I!!PDF-E&type=items.

Li, Li Erran, Z. Morley Mao, and Jennifer Rexford. "Cell SDN: Software-Defined Cellular Networks." White paper, Bell Labs (2012). Accessed Feb. 16, 2014, http://www.bell-labs.com/user/erranlli/publications/CellSDN-TR12.pdf.

Mendonca, Marc, Bruno Astuto A. Nunes, Xuan-Nam Nguyen, Katia Obraczka, and Thierry Turletti. "A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks," May 24, 2013. Under review at *IEEE Communications Surveys and Tutorials*. Accessed Feb. 23, 2014, http://hal.inria.fr/docs/00/82/50/87/PDF/SDN_survey.pdf.

Nuechterlein, Jonathan S. and Philip J. Weiser. *Digital Crossroads: American Telecommunications Policy in the Internet Age*. Cambridge, MA: MIT Press, 2005.

Open Networking Foundation. "Software-Defined Networking: The New Norm for Networks." White paper, Apr. 13, 2012. Accessed Feb. 16, 2014, https://www.opennetworking.org/images/stories/downloads/white-papers/wp-sdn-newnorm.pdf.

Robertson, Jordan. "Google+, Candy Crush Show Risk of Leakiest Apps." *Bloomberg*, Jan. 29, 2014. Accessed Feb. 16, 2014, http://www.bloomberg.com/news/2014-01-29/nsa-spying-on-apps-shows-perils-of-google-candy-crush-.html.

Rusli, Evelyn M. "Buy Signal: Facebook Widens Data Targeting." *Wall Street Journal*, Apr. 9, 2013. Accessed Feb. 16, 2014, http://online.wsj.com/news/articles/SB10001424127887324504704578412960951909032.

Sengupta, Somini. "Trust: Ill-Advised in a Digital Age." *New York Times*, Aug. 11, 2012. Accessed Feb. 16, 2014, http://www.nytimes.com/2012/08/12/sunday-review/bruce-schneier-an-avatar-of-digital-distrust.html.

Shine, Dave. "Intro to Hadoop." Speech before the Orlando.net User Group, Apr. 18, 2013.

Stallings, William. *Data and Computer Communications*, 9th Ed. Upper Saddle River, NJ: Prentice Hall, 2010.

Tellabs. "How the Smart Mobile Internet Transforms Your Business." White paper, June 2011. Accessed Feb. 16, 2014, http://info.tellabs.com/rs/tellabs/images/tlab_smartmobleinternet_wp_742360.pdf?mkt_tok=3RkMMJWWfF9wsRonuq/MZKXonjHpfsX96+4pWLHr08Yy0EZ5VunJEUWy2YIGSdQhcOuuEwcWGog81AlUFuGXbw==.

Troianovski, Anton. "AT&T Move Signals End of the Copper-Wire Era." *Wall Street Journal*, Nov. 7, 2012. Accessed Feb. 16, 2014, http://online.wsj.com/news/articles/SB10001424127887324439804578104820999974556.

———. "Phone Firms Sell Data on Customers." *Wall Street Journal*, May 21, 2013. Accessed Feb. 16, 2014, http://online.wsj.com/article/SB10001424127887323463704578497153556847658.html.

Vascellaro, Jessica E., Sam Schechner, and Spencer E. Ante. "New iPhone to Support LTE." *Wall Street Journal*, Sept. 7, 2012. Accessed Feb. 16, 2014, http://online.wsj.com/news/articles/SB10000872396390443819404577637903902952754.

Wallace, Steve, Uwe Dahlmann, Ron Milford, and Chris Small. "Openflow in a Day." Presentation at NANOG58, New Orleans, LA, June 3, 2013. Accessed Feb. 23, 2014, http://www.nanog.org/sites/default/files/mon.tutorial.wallace.openflow.31.pdf.