User-Centric Networking: Putting the "I" in Internet

Ross Teixeira
Princeton University
rapt@cs.princeton.edu

Jennifer Rexford
Princeton University
jrex@cs.princeton.edu

ABSTRACT

The COVID-19 pandemic enables a new twist on how we teach computer networking. Instead of a *bottom-up* or a *top-down* approach, we propose a *user*-centric approach to empower today's remote students, starting at students' local networks and expanding outward across all layers. Through hands-on measurements from their own locales, and discussions of real-world events and public policy about the Internet, students can gain a first-hand understanding of their place in an increasingly virtual world. Studying and measuring popular Internet applications helps students understand what determines the performance (or reliability, or security, or privacy) they see, while comparing and combining measurement results with their classmates can reveal the heterogeneity of the Internet as well as its underlying structure. Furthermore, discussion of recent news articles about the Internet under COVID-19, coupled with case studies of how the Internet fared during past major events, provides a unique way for students to grapple with important public policy questions. Together, these ideas form a radical approach to networking education that may persist long after lockdowns are eased.

1 INTRODUCTION

> "The best thing to do is give them more things to take apart so they can see how things work on the inside. Give them tools, and teach them how to use those tools."
>
> – *Grant Imahara*

For most of today's students, the Internet has been an inexorable part of their lives for as long as they can remember. The Internet is their immanent educator and entertainer, both a window and a microphone connecting them to the global community around them. Despite having kept its fundamental architecture for decades, the Internet maintains that global community through natural disasters, wars, and pandemics. Indeed, the Internet's stability as global communications infrastructure makes it a powerful lens for studying the effects of these major events, and a great motivator for students learning in an era of unprecedented uncertainty and grappling with how to define their own roles in improving the world around them.

With billions staying home to attend school lectures, work meetings, and social events, the Internet has supported the excess demand during COVID-19 with remarkably few hiccups. However, this does not mean that everyone has equal opportunity to utilize it. With many students experiencing poor home Internet conditions, educators face a difficult task to ensure every student can access course materials and resources remotely. Worse, even with perfect connectivity, many educators still fear that remote teaching spells disaster for engagement in two respects: 1) engaging personally with students is much more challenging, and 2) students will not have the same ability to engage with networking hands-on as they would with in-person classrooms or labs.

On the contrary! We believe the current pandemic—and the large-scale move to online instruction—offers networking educators a powerful opportunity to teach students networking by leveraging their diverse perspectives as members of the Internet and society at large, by having students conducting Internet measurements from their homes and engaging in discussions about Internet public policy. In particular, we propose four key ideas for networking educators to take advantage of this coming year, which we describe in detail in this paper:

- A diverse set of students can use their direct experiences with their home connectivity and familiar Internet applications to enable personal, hands-on learning that was not possible before;
- The heterogeneity of Internet conditions among geographically dispersed students provides an excellent measurement lens to observe global network conditions;
- The prominence of the Internet (and popular services like Zoom) in the news during the pandemic enables students to grapple with important and timely public policy questions;
- The robustness of the Internet under COVID-19 (and other major events) provide evidence of the foresight and ingenuity of the Internet's architects.

Nowadays, students can interrogate many aspects of the Internet from their own laptops, using both low-level tools of the trade (e.g., Nmap, wget, traceroute, iperf, tcpdump, and more) and familiar high-level applications (e.g., email, web browsing, Netflix, Zoom, and more). For students stuck at home, measuring properties of their home network and access link will reveal network properties far more diverse than those of students normally on campus, allowing for engaging class discussions. In addition, we posit that studying familiar applications will increase engagement and motivation for students, as the networking lessons are grounded in their everyday experiences with the Internet. Naturally, we expect these home measurements to be just as good as a "hands on experience" (if not better) than any students might perform in a traditional classroom or lab.

To realize these measurements in a curriculum, we propose a "user-centric" approach to teaching networking, in which layering is introduced early on and all layers are studied together. Topics are introduced in order of "proximity" to the student, beginning at the home network and expanding to include global network properties and resource allocation among many connected users.

Of course, a hands-on approach runs the risk of exposing students to the minutiae of networking at the expense of covering the concepts. We believe that a networking course can (and should) cover the details while also rising above them. In fact, experiential learning about the "nuts and bolts" can help motivate the students to learn the important concepts and truly internalize them. Indeed, we propose combining hands-on exercises, all done from the students'

own computers in their own locales, with lectures and programming assignments that cover the material in a more traditional and structured way (albeit in a different order than usual).

On the surface, conducting experiments from user machines might seem to miss out on important networking topics "lower" in the networking stack or "deeper" in the core. However, we argue that hands-on exercises can peer down the stack and across the Internet to touch on a surprisingly broad set of networking topics. In addition, discussing public policy topics that arise in the news, coupled with case studies of how the Internet fared during other major events, can expose students to aspects of computer networking that are less readily visible from their home networks.

A user-centric curriculum puts the student experience at the focal point of the class. In doing so, it must balance this goal with concerns of student privacy and disparity in Internet connectivity, to empower students without discouraging them. These concerns illuminate both the power of a user-centric education, and the conversations that must take place to ensure an inclusive classroom experience. With earnest consideration, user-centric networking may outlive lockdowns as a fundamental aspect of future networking courses.

We first present a progression of hands-on exercises (Section 2) and suggested discussions of world events (Section 3). We then discuss challenges in realizing the curriculum (Section 4), describe the future potential of user-centric networking post-COVID (Section 5), and conclude (Section 6). The specifics of integrating the exercises and discussion topics, along with lectures and programming assignments, into a full curriculum are left as future work.

2 QUESTIONS FROM THE EDGE

We propose creating a collection of hands-on exercises that ask seemingly simple questions, and take the students through tools and experiments they can run on their own computers to come to answers. Throughout, students can compare and combine results with other students in different locations.

2.1 The Student's Local Environment

At the start of the course, the students learn about their own networking environment (their "home" network, whether in their actual home, or a dormitory, or a public library or community center). In the process, they become familiar with traffic-monitoring tools (e.g., Wireshark or tcpdump), the network configuration of their laptop (e.g., ifconfig), and more. (For students using public computers without root access, the staff can instead supply sample packet captures for traffic monitoring.)

How does my computer connect to the Internet? The students turn off their Internet connectivity (e.g., by unplugging the Ethernet cable or turning off WiFi), and monitor and analyze the traffic involved in bootstrapping their computers. This allows them to learn about DHCP, and to see use ifconfig to see the interface's MAC address, as well as the IP address, subnet mask, DNS server, and gateway learned via DHCP.

What else is in my home network? Students have the opportunity to understand their own home network. They can scan their home network (e.g., using Nmap [1]) to learn what other devices are connected to their home networks, and report what they learn.

How do multiple computers in my home use the same Internet connection? The students can visit sites like https://www.whatismyip.com/ to learn the public IP address associated with their home network connection, and how it differs from the (private) addresses assigned to their computers via DHCP. The students can learn about Network Address Translation (NATs). If they have the credentials for their home router, they can log in to the home router to see more information about the devices connected to the home network.

Why does my WiFi coverage vary so much? Most students will access the Internet using WiFi. They can report how many different WiFi access points they are able to see from different locations in the home, and also report WiFi performance in terms of the number of "bars" visible and performance tests (e.g., using iperf or a SpeedTest site). They can produce a "map" of where WiFi performance is good (or bad) in their home and consider how it relates to proximity to the access point, the number of other APs nearby, the number of other WiFi-connected devices, and the equipment and physical structures around them.

2.2 Popular Internet Applications

With an understanding of basic Internet connectivity, the students can start exploring the underlying client/server traffic that powers common applications like email, Web browsing, video streaming, video conferencing, and peer-to-peer applications. The goal is to get a basic understanding of the multiple layers of the protocol stack and how they work together to offer Internet services.

How are my emails sent, received and retrieved? Have students pair up and send each other an email from a school email account to a personal account (students can create a new account for this experiment if desired). Each student can then log into the Web clients for their school and personal emails, and view the email headers. By observing the "Received" headers, each student can learn which servers are involved in handling the emails. Note that the student's computer only uses HTTPS traffic to send and receive emails through the browser, as the actual email transfers are handled separately by the email providers. A student can then log into their email via a local email client (Apple Mail, Thunderbird, etc.) and observe the IMAP or POP3 connections between their computer and the service provider. They can observe the asynchronous nature of POP3 email traffic: the client only pulls email locally every few minutes, while it appears immediately when accessing through HTTPS.

How does my browser download a web page? Students can download a simple Web page (using their browser or a tool like wget), preferably visiting a Web site that supports HTTP (instead of HTTPS) to see the HTTP messages on the wire without encryption. They can see the DNS query, followed by the TCP connection with the HTTP request and response messages. They can see the automatic download of embedded images referenced in the HTML file. If an HTTPS website is desired, Firefox and Chrome can output SSL keys via a command-line argument for use in Wireshark [2], or students can use an HTTPS man-in-the-middle proxy like mitmproxy [3] or Fiddler [4].

How does my computer stream a video? The students can download streaming video (e.g., from Netflix, Hulu, YouTube, Amazon Prime Video) and observe the sequence of video chunks according to the video's encoding quality. They can manually select different encoding formats or quality levels, and monitor the resulting differences in chunk size and frequency, buffering, or other quality-of-experience (QoE) metrics through Wireshark or provided by the video stream client [5]. Students can also compare the server's recommended encoding quality with their actual experience watching each encoding quality, and discuss what features may be considered by the server when recommending a stream quality.

How do I participate in a video conference? Students can monitor the video traffic while participating in a video conference (such as the lecture for their computer networking course!). They can determine whether the video traffic is centralized (sent to a central server or set of servers) or decentralized (sent directly between call participants). They can try capturing various scenes with their webcam (e.g., a static image, dynamic movement, multiple colors, etc.) and observe how different scenes affect traffic rates. They can note disruptions in their QoE and speculate as to the cause. Students can also examine the marginal increase in bandwidth or decrease in QoE for each student that joins a call. Finally, they can also try multiple video conferencing tools and compare how they handle varying webcam scenes and numbers of call participants.

How do peer-to-peer applications work? Students can download a staff-provided torrent or join a Matrix chat to understand decentralized networks. They can build a map of the other students they have direct edges to in the decentralized graph. In a Matrix chat, pairs of students can send messages to each other and observe how long it takes for each message to traverse the network.[1,2]

Networking vs. computation. Some students may notice high CPU usage (whirring fans, slowdowns) when running certain Internet applications such as video streaming or web conferencing. By observing network traffic from the application and modifying the content being sent/received on the network, students can investigate the relation between network traffic and CPU utilization. There are many ways this experiment might play out. If sending a complex webcam scene increases both network traffic sent and CPU usage compared to a static scene, a student may theorize that sending large amounts of data uses a lot of CPU. If CPU usage increases but network traffic does not increase significantly, the student may speculate reasons for this, such as a CPU-intensive video compression algorithm. These effects can also be compared across video conferencing applications to see how, for example, Zoom and Teams handle network traffic/compression differently.

[1]There is an ethics issue for students who do not wish to reveal their IP addresses.

[2]We also considered running a custom Tor network across students' computers, but there are significant barriers to this idea. First, students cannot run relays behind NATs without port forwarding. Also, students should not run a Tor exit node, as this puts them at risk if other students access illegal content through the network. (Note that a student Tor network is isolated from the main Tor network, so existing hidden services cannot be accessed.) However, it is definitely worth having a class discussion on the ethics of services like Tor and operating systems like Tails for preserving privacy and anonymity.

2.3 Underlying Internet Infrastructure

Next, the students learn about the underlying infrastructure for directing users to their services—including name resolution (DNS), content routing (CDNs), and network routing. Comparing results with other students provides a glimpse into the distributed infrastructure of name servers, CDN servers, and routers underlying the delivery of Internet services.

How are domain names resolved into IP addresses? Students can explore the domain name system using tools like dig and nslookup. They can perform queries on popular site names and compare results with other students. They can also repeat queries to see how DNS caching reduces lookup time. Students can also monitor their Internet traffic for a period of time, and note the names of servers (as seen in DNS queries) their computer contacts. The students can write a program to "join" the DNS name with the subsequent data traffic to report traffic volumes by domain name. Some results will be as expected (e.g., popular sites like google.com, facebook.com, or netflix.com) while others may be less familiar (e.g., advertising sites).

How do Content Distribution Networks deliver content? The students can download a Web page that is hosted (or has its images hosted) by a Content Distribution Network (CDN). The students can look at the page source to better understand how the CDN works. Students in different locations can download the same Web page and compare differences in which CDN edge servers their browsers contact. They can run this experiment multiple times over several days, and find that the number of servers they see may be correlated with the proximity of students' homes to CDN servers [6]. They can analyze statistics like round-trip time (collected via ping, or passively from the packet traces) to estimate how far away the CDN server nodes are from them—and compare with their classmates. The students can discuss how CDNs might decide where to place their edge sites and how to decide which replicas should serve different clients.

What path does my traffic take through the Internet? Students can understand what traceroute does and how it works. First, they can run traceroutes for a single server and visualize the resulting packets with Wireshark. Then, they can study the traceroute results, to understand what networks their traffic traverses en route to the server. By combining results with those of other students, they can see a "sink tree" to a common destination. The students can look at the domain names in traceroute, and map IP hops to Autonomous Systems (ASes) based on IP-to-AS mappings derived from BGP data, to understand what ASes the paths traverse. Students can run traceroute to each other's IP prefixes to see whether routing is (or is not) symmetric. The students can also analyze data from public traceroute and BGP routing servers to measure the paths from remote vantage points to their own IP prefix, and compare with traceroute probes they send to those remote servers. Finally, students with a smartphone can run traceroutes from their phone, and compare them to traceroutes ran from their home network to the same destination, to understand how cellular networks route packets.

2.4 Distributed Resource Allocation

Next, the students conduct experiments that illustrate the effects of resource-allocation decisions on network performance.

How does TCP congestion control affect application performance? The students can run Wireshark on their own Internet traffic, and generate time-series plots of the evolution of different TCP connections. This allows them to see how TCP throughput starts small and then ramps up, until packet loss or delay triggers a decrease in the congestion window. They can reason about the effects on Web performance, particularly for small web objects. They can run experiments with larger data transfers with different servers to experience how TCP throughput relates to round-trip time, and connect these observations to their earlier experiments on the proximity of CDN servers.

How does TCP share bandwidth across connections? The students can run multiple connections at the same time and see how they affect each other's performance. For example, they can download a web page with different numbers of concurrent connections (to download embedded images) and determine which configuration offers the best performance. The students can also download data concurrently from different servers with different round-trip times (RTTs) and compare the bandwidth shares between different connections. They can also discuss how they think their operating system should divide bandwidth among multiple applications running on the same user device.

How should my home network share bandwidth across users? The students can explore how other activities in the home (e.g., a roommate or family member participating in a Zoom call or watching Netflix) affect performance. They can discuss what kinds of policies they think the home router could impose to differentiate traffic based on its "importance" (e.g., work-related Zoom call vs. Netflix streaming) or its sensitivity to loss or latency (e.g., videoconferencing vs. Web browsing).

How do video streaming services adapt to TCP throughput? The students can return to their earlier experiments with video streaming services and see how TCP performance triggers changes in the video quality. They can also see how some performance disruptions in TCP are *not* visible in the streaming application, due to playout buffering. Students can discuss the multiple control loops (TCP and the video quality adaptation) and how they interact.

3 INTEGRATING WORLD EVENTS

COVID-19, as well as other major world events, impact the Internet and are themselves shaped by the Internet. These events provide a unique opportunity to showcase important public policy issues, while also offering instructive examples of Internet protocols operating under extreme circumstances. Students can read and discuss news articles, measurement studies, and policy reports about these events to complement the hands-on exercises in the previous section. In particular, these events allow a networking course to delve into privacy and security issues that are harder to address through hands-on exercises.

3.1 COVID-19 Internet Policy Questions

Stay-at-home orders have exposed the vast consequences of the worldwide disparity in Internet connectivity, bandwidth, and the ability to share and access information freely without barriers or censorship. It is important to teach students about the numerous public policy issues involving the Internet, so they are able to engage in civil endeavors on improving internet access for everyone. To supplement the hands-on assignments in the previous section, students can read articles about a number of Internet policy issues that arise under COVID-19 and discuss them in class.

Service overloads. While many remote education and telework platforms have scaled rapidly to support extra demand, some have experienced outages. In China, back-end servers for major platforms from Baidu, Tencent, and others were temporarily unable to keep up with demand [7].

Digital divide. The "digital divide" of Internet connectivity is experienced disproportionately by rural, low-income, and minority communities. Many students are facing difficulties learning remotely due to not having access to adequate, or any, Internet at home [8]. Some students may also not have a personal computer, and must share with others in their home or use a public machine (complicated by the fact that libraries and other services have been closed). In response to these issues, some ISPs have offered 4G subsidies for students [9], while some school districts have resorted to physically mailing thousands of pages of course material to each student [10].

Limited broadband service options. Collecting accurate data on broadband coverage is essential to closing the divide, and students are able to test their own experience against government estimates. In the U.S., for example, students can check which ISPs provide coverage to their home address according to the Federal Communications Commission's (FCC) official maps. Then, students can visit each ISP's website and input their addresses into the ISP's "Check Availability" page (if one exists), and compare the results to the FCC's maps. Such a methodology has been used to study the accuracy of FCC coverage maps at small scale, and students are able to replicate this for their own home coverage [11]. The students can discuss how limited options for broadband connectivity affect different communities, and how ISPs with near monopolies might take advantage of their roles.

Net neutrality. Net neutrality laws require ISPs to treat all network traffic equally, and prohibit ISPs from blocking, throttling, prioritizing, or charging extra for certain lawful traffic. One of ISPs' primary arguments *against* net neutrality laws is the need for ISPs to prioritize emergency traffic over general entertainment traffic, citing fears that a significant increase in entertainment traffic would harm the ISPs' ability to provide high-speed connectivity to emergency services. However, while internet traffic has raised considerably during the pandemic, outages have been predominantly local and slowdowns can likely be attributed to home router saturation [12, 13]. Thus, the pandemic has provided evidence that net neutrality harms the Internet less than critics suggest.

Censorship. A handful of countries block certain types of content from being accessed on the Internet, with exceptions for certain contexts, such as academic institutions. With students and educators forced to stay home, censorship has become a barrier to

education. In China, a bioinformatics lecturer was cut off in the middle of class for presenting content that violated China's Internet regulations, while other biology, history, and politics courses have experienced censorship, even for phrases historically used by the Chinese government [14].

Contact tracing and surveillance. Many countries are considering variants of mobile contact tracing applications that track the spread of COVID-19 [15]. Contact tracing approaches differ in their depth of surveillance. Some privacy-preserving approaches use short-range Bluetooth [16, 17] or radio signals from cell towers [18] to identify close interactions between people without revealing identities or tracking locations. Other approaches involve fine-grained GPS tracking [19–22]. In addition, companies have joined the race to publish data about the effect of stay-at-home orders on transportation and the economy, with varying degrees of preserving privacy of individuals [16, 23–25]. Some fear that surveillance during the pandemic could normalize public surveillance in other situations, a long-term privacy issue. Publishing data from personal surveillance can also become a national security issue, such as when the fitness tracking app Strava released a global map of user data that revealed the locations of sensitive U.S. military bases [26].

Disabling paywalls and open access research. Many academic journals have removed paywalls on their libraries during the pandemic, to allow researchers and others to easily access academic articles from home [27]. While open access to COVID-19 studies greatly accelerated progress in fighting the pandemic, the benefits of open access extend to every discipline; even the ACM had opened access to its library until July 1 [28]. Major universities are already pursuing open access agreements with top publishers like ACM, Elsevier, and Springer, and ACM has hinted (on Twitter) about its goal to open its library for all within five years [29]. The pandemic has clearly illustrated the benefit of enabling access to quality research for everyone, and may be the catalyst that sparks further expansion of open access to research.

Privacy/security problems in Zoom. Zoom had long claimed to provide end-to-end encryption of their video traffic, traditionally understood to mean that video call data could only be read by the call's participants and no one else, including Zoom. However, additional scrutiny was applied to Zoom after its usage skyrocketed during the pandemic, and security researchers found this claim to be misleading. Calls were only "end-to-end" between participants and Zoom's servers, but Zoom was able to read traffic data [30]. Encryption keys were being sent to servers located in China, where Zoom's engineering team is predominantly located, which some consider to be an issue of national security. Lastly, the encryption mode previously used by Zoom is known to preserve patterns in data, which can easily be spotted in encrypted images or videos. Citing this extra scrutiny, Zoom has now drafted a plan to provide true end-to-end encrypted video conferencing [31]. Here, it is important to teach students to be critical of popular services and gain an intuition for understanding and even exposing critical vulnerabilities.

Online voting. With public health officials decrying in-person voting, many governments are turning to online and mobile voting platforms as a solution. However, online voting comes with many problems of its own. Ensuring all desirable properties—including ballot secrecy (no one can coerce or observe your vote), single-vote verification (each person casts their own, single vote), and security (votes are not susceptible to tampering or suppression)—is very difficult to achieve in an online voting scheme [32, 33]. Researchers have demonstrated network denial-of-service (DoS) attacks, weak encryption, or other tampering and data leaks in prior online voting systems in several countries [34–36]. Most importantly, elections depend on public trust that the voting system works as intended, so it is useful for students to learn how secure online voting works and why truly secure and verifiable online voting is still years away.

3.2 Other Major Internet Events

The Internet has weathered many other major events before the COVID-19 pandemic. Some world events caused the Internet to be used in new ways, and others cause parts of the Internet to become unavailable due to physical damage, cyber attacks, or government censorship. Through case studies of world events, students can explore a wider range of networking issues in a social or political context. In some cases, an event "fits" naturally at a particular point in the curriculum (e.g., high-profile BGP outages as part of a discussion of Internet routing). In other cases, an event may arise many times throughout the semester (e.g., the 9/11 terrorists attacks in the U.S.) to illustrate how various protocols or services operate.

Wars and terrorist attacks: The 9/11 terrorist attacks [37] provide an opportunity to discuss a wide range of computer networking topics. These include changes in application workloads (e.g., a shift to instant messenger and news sites), the Domain Name System (with South Africa's top-level domain (TLD) server, located in NYC, going offline), scaling up content delivery (with CNN editing its home page to fit in a single packet, and reenlisting Akamai's CDN service, to accommodate an unprecedented surge in demand), and network reliability (including problems with refueling the power generators in Internet colocation facilities in lower Manhattan).

Natural disasters and accidents: Natural disasters like the Taiwan earthquake of 2007 [38] and Hurricane Sandy (in the U.S.) [39] provide an opportunity to observe the effects of damage to the Internet infrastructure (and the impact of damage to the power grid) as well as the role of the Internet in search and recovery efforts. Similar to natural disasters, major accidents such as the Middle East fiber cut (the 2008 submarine cable disruptions) [40], the Baltimore Tunnel Fire (the 2001 fire that destroyed many fiber-optic cables) [41], and others [42] also highlight how the Internet is not always as robust as we expect, due to the concentration of Internet capacity in a single location. Students can discuss how climate change may put the Internet further at risk [43].

Political upheavals: Events like the Arab Spring provide an opportunity to discuss the role of the Internet in enabling rapid encouragement and organization of protests (e.g., through social media like Twitter) [44], while also discussing government censorship (including governments shutting down the Internet with the goal of stifling the protests and reducing international visibility) [45].

Major Internet security incidents: Significant security events provide an opportunity to study network protocols by understanding their vulnerabilities. For example, BGP incidents like the China

Telecom interception [46] and the Pakistan Telecom YouTube outage [47] go naturally with the treatment of Internet routing, as they illustrate how erroneous BGP announcements can have global consequences. Other high-profile incidents—like the Morris worm, the Mirai botnet, and the Kaminsky DNS vulnerability—provide opportunities to study other aspects of network security.

4 DISCUSSION AND CHALLENGES

Here, we explore challenges and begin conversations towards realizing this proposal as a curriculum that respects and empowers students from all backgrounds.

4.1 Heterogeneity and Inclusive Pedagogy

User-centric networking reaches its full potential when students from all locations and backgrounds are able to share their individual experiences of the Internet, contribute their local measurements to a global class pool, and engage in discussions of current and past worldwide events with their peers.

While we have every intention of highlighting the benefits of a diverse classroom through user-centric networking, we must also acknowledge the harms that such an emphasis on individual diversity can cause students. Many of the measurements we suggest involve the performance of students' connections, including overall bandwidth, interference with roommates or family members, application QoE, proximity to CDN servers or other classmates, and location, which may be correlated with other demographics. Many measurements make assumptions that students have access to a personal laptop with root access for collecting network traffic. We propose that students collaborate simultaneously for P2P and video conferencing measurements, which is difficult for students who live across many time zones. And we engage students in discussions about world events which may have affected, or continue to affect students, their families, and their communities. A student who is continually asked to examine the disparity between themselves and their classmates without contextualizing it, or who feels undue pressure to be the spokesperson for their background to the class, may quickly become discouraged by these "stereotype threats."

We believe these challenges do not diminish the value of a user-centric education. Rather, they represent crucial, oft-overlooked aspects of inclusive teaching which must be considered when building a curriculum on the merits of heterogeneity. Below, we present potential directions towards addressing these concerns. We recognize that greater solutions will require earnest conversations among members of our community, especially with and among students, and we hope our proposal is only the beginning.

Upfront expectations. A user-centric networking course must be explicit about the contents of the course before students enroll. Instructors should make students aware that they will be expected to conduct measurements from their own computers to the extent possible, and that their measurements may be shared with the class (more on opt-in sharing below). Instructors should also provide examples of the real-world events and public policy issues that they intend to cover, and why these benefit students.

Anonymous and opt-in measurement sharing. An overarching theme of user-centric networking is to use the heterogeneity of student measurements as a tool to build a bigger picture of Internet connectivity. However, some students may wish to keep info about their location or connectivity private. We suggest that instructors anonymize the measurements of students to the extent possible when presenting them to the class, or aggregating measurements such that individual measurements cannot be determined. In addition, sharing measurements with the class should be opt-in by default, so that students who wish to maintain privacy can do so without the stigma of going against "normal" or "expected" behavior.

On the other hand, we hope that some students may be excited to present their measurements to the class, and especially about insights they gain about their local environment. We feel a user-centric course should encourage this enthusiasm and allow presentations. Some measurements, such as understanding how popular applications work, can be presented without revealing details of a students environment; these could be graded individual or group presentations. Data that can be correlated with a student's environment can still be presented, as long as these presentations are opt-in, ungraded, and moderated to connect students' findings to broader themes of the course.

Laptop loaner programs. Some schools maintain a reserve of laptops that students can borrow for a period of time. This is far from a permanent solution, as not every school maintains a loaner program, and demand for loaner laptops has greatly increased due to closures of public libraries and learning centers during the pandemic. But students should be made aware of the school's loaner program if one exists.

Alternative sources of data. For students who are unable to run their own measurements, course staff can prepare alternative sources of data, such as PCAP files, HAR files for web activity, etc. Students who experience technical issues conducting measurements may also appreciate having these examples available as a backup. Provided examples have the additional ability to be "cleaned" by staff to remove extraneous information, which may benefit all students as examples of expected (or unexpected!) behavior during measurements.

Engaging students broadly with the "digital divide." Holding class discussions on the "digital divide" is a good way to get all students thinking about the problems that arise when people do not have access to adequate broadband internet, without calling attention to individual students or their specific environments. (See Section 3 for further info on the "digital divide.")

4.2 General Pedagogy and Logistics

In addition to heterogeneity, we consider two general aspects of user-centric networking to aid its adoption.

Hypothesis testing. The *result* of a measurement is only half of the learning process: equally important is how students *reason* about a measurement before and after observing it. We propose structuring measurement exercises such that students must first hypothesize about the results of a measurement and the factors that might cause or influence the results. Then, after conducting a measurement, students should discuss whether their results matched their hypotheses and why or why not, as well as what other factors may have been involved. Students should consider how running

measurements with alternate environments or network conditions would affect the results. Students can also design follow-up measurements that could isolate the effects of specific causal factors, to provide evidence for (or against) their effects.

Hypothesis testing forces students to think critically about networking concepts and how their environment interacts with the network. It also gives instructors more opportunities to gauge how well students are learning the course material. Finally, it aids inclusive learning by having students speculate about conducting measurements in alternate environments. This is especially beneficial if combining measurements from students produces homogeneous results, which may occur if students are located in a small number of similar locations, or if many students are analyzing staff-provided measurements.

We recommend that when grading students' hypotheses, instructors should award the majority of points to the depth of students' thoughts about the outcome and potential causes, and a smaller amount to whether the student gets the right answer. This would encourage students to think deeply without stressing over being perfectly accurate.

Partial integration. There is still much work remaining to create a complete user-centric curriculum which covers all topics of a traditional networking course in depth, supported with student measurements and discussions of public policy and world events. Certain topics, such as L3 routing protocols, SDN, and network management, are difficult to measure from the edge, and may benefit from more traditional hands-on projects like simulators. Also, introducing students to layers in a user-centric curriculum will require careful calibration. We leave these challenges as future work.

However, educators need not wait for a complete user-centric networking curriculum in order to start adopting these pedagogical techniques. There is ample room for user-centric exercises and discussions in existing networking courses, and we encourage educators to ponder how their courses might support user-centric ideas.

5 LOOKING FORWARD: USER-CENTRIC NETWORKING POST-COVID

We now consider how user-centric curricula may persist in networking education, long after lockdowns ease and universities resume normal campus life.

5.1 On-campus Teaching

Many of our proposed measurements are unaffected by the locations of students, or can be adapted to support measuring interesting properties of campus networks. Our goal is still to show students how their individual, unique measurements can be combined to produce an interesting, broader picture of connectivity.

Student's local environment. Students can test the throughput of their lecture hall's WiFi by having every student download a large file or stream 4k video simultaneously. Each student can measure their throughput on their laptop and estimate the total throughput of the class. Students can scan for the number of access point BSSIDs in the lecture hall. They can re-attempt the experiment while all connecting to the same access point's BSSID and observe if throughput decreases. In addition, students can study WiFi access points around campus: for example, students can explore different parts of campus and measure WiFi connectivity in terms of number of available access points and signal strengths, and look for surprising areas with poor connectivity.

Popular internet applications. Measuring popular internet applications (email, web, video streaming, video conferencing, P2P) can be done regardless of a student's location. For peer-to-peer networks, students would now study properties of the campus network.

Underlying internet infrastructure. Students can reverse the "sink-tree" from remote learning, and instead run traceroutes to different servers worldwide to create a "source-tree" from campus. Students can observe the number of uplinks that connect the university to the Internet, and who the uplinks belong to. A representative from the campus' network management team can give a guest lecture about the campus network and current projects or issues they are working on.

Distributed resource allocation. Individual measurements (such as measuring web traffic with concurrent HTTP connections) work unchanged, while students may collaborate or ask their roommates to help with performance measurements across multiple devices on the same access point.

Integrating world events. Finally, student discussions on disparities in Internet connectivity, public policy issues surrounding the Internet, and major events translate naturally to in-class discussions.

5.2 Bursting the Bubble

Finally, we examine how user-centric networking education can extend beyond the course, the school year, and universities altogether.

Collaboration across universities. With students living on campus, the campus becomes a single, giant vantage point for broader network measurements. However, there is an enticing opportunity for students from different campuses to interact and collaborate on Internet measurements through their respective networking courses. We believe this is an excellent way to break students out of the bubble of their campus environment, ideally by collaborating with students at universities far and very different from their own. In the far future, one could imagine a platform that collects and displays longitudinal, semesterly measurements from students at universities around the world.

Holiday/summer measurement exercises. There are multiple reasons why students might want to continue conducting measurements once the semester ends. Students who find their networking course particular interesting may look for ways to keep learning and participating in the networking community as researchers and TAs, or through coding side projects. Also, students from diverse locations may be inspired to take the knowledge they learn during the semester and apply it to understanding their home environment. We believe that developing a set of measurements that students can perform at home on their own would greatly benefit the networking community, even for existing courses taught using a more traditional curriculum.

Massive Open Online Course. Millions of people, particularly adults, are already studying and earning degrees online through MOOCs on platforms like EdX, Coursera, and MIT OpenCourseWare. A MOOC would provide a broad platform for conducting diverse, aggregated user measurements. Moreover, a user-centric networking MOOC would give people the tech literacy they need to understand their own Internet connectivity and the Internet public policy issues that affect them and others less privileged, making them more informed citizens and voters.

In particular, in addition to networking for CS majors, we believe there is room for an Internet MOOC that targets a more general audience, while still incorporating user-centric network measurements. The difficulty and the depth of material should be adjusted appropriately.

6 CONCLUSION

> "Many people say that they became successful by being in the right place at the right time. The trick is to get yourself to the right place at the right time, have the necessary skills, and be available for opportunity. All of these things are totally within your control."
>
> *– Grant Imahara*

Network engineers around the world deserve utmost praise for maintaining an incredibly robust system that has kept us connected in the face of such dire isolation and concern for those we love. Through their efforts, we define our lives as family members and friends in this time, and as networking researchers and educators throughout our lives. Certainly for each of us, there was a budding moment of discovery running traceroute or peeking into Wireshark, and glimpsing at the complexity below the surface. It is those wondrous moments, those sparks when you first realize your place in a worldwide network, that kindle a life dedicated to improving it, and to ensuring that everyone has the knowledge and ability to discover those sparks for themselves.

We each have changed plenty since we felt those initial sparks, and the world around us has changed, too. As with the Internet, everyone deserves the chance to realize their place in the world and how to improve it. We researchers work to make the Internet faster, more robust, more accessible, and various other metrics that can all be described succinctly as, "better." In times of great change, it is imperative that we reflect on how to best use our skills to better the world; here, we illustrate that educating and inspiring new networking experts is a viable and modest start. While it is commonly known that the Internet architecture changes little, we can learn much by applying that knowledge to a changing world.

ACKNOWLEDGMENTS

We greatly thank Shriram Krishnamurthi for the ideas of studying the marginal costs of video conference participants, network vs. computation experiments and hypothesis testing. We thank Justine Sherry for help on framing the proposal. We thank Jèrèmie Lumbroso for conversations on heterogeneity and stereotype threat. We further thank Mary Hogan, Xiaoqi Chen, Satadal Sengupta, and our anonymous reviewers for their helpful comments and suggestions. We thank you for reading this.

REFERENCES

[1] G. F. Lyon, *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*. Sunnyvale, CA, USA: Insecure, 2009.
[2] "Decrypting TLS browser traffic with Wireshark – the easy way!," March 2019. https://redflagsecurity.net/2019/03/10/decrypting-tls-wireshark.
[3] "mitmproxy - an interactive https proxy." https://mitmproxy.org/.
[4] "Fiddler - web debugging proxy." https://www.telerik.com/fiddler.
[5] A. Mondal, S. Sengupta, B. R. Reddy, M. J. Koundinya, C. Govindarajan, P. De, N. Ganguly, and S. Chakraborty, "Candid with youtube: Adaptive streaming behavior and implications on data consumption," in *Proceedings of the 27th Workshop on Network and Operating Systems Support for Digital Audio and Video*, NOSSDAV'17, (New York, NY, USA), p. 19–24, Association for Computing Machinery, 2017.
[6] A.-J. Su, D. R. Choffnes, A. Kuzmanovic, and F. E. Bustamante, "Drafting behind Akamai: Inferring network conditions based on CDN redirections," *IEEE/ACM Trans. Netw.*, vol. 17, p. 1752–1765, Dec. 2009.
[7] "Is the Internet resilient enough to withstand coronavirus?." https://www.internetsociety.org/blog/2020/02/is-the-internet-resilient-enough-to-withstand-coronavirus/.
[8] "Doing schoolwork in the parking lot is not a solution." https://www.nytimes.com/2020/07/18/opinion/sunday/broadband-internet-access-civil-rights.html.
[9] "Online classes in coronavirus-hit China leave kids without Wi-Fi struggling." https://www.scmp.com/abacus/culture/article/3064852/online-classes-coronavirus-hit-china-leave-kids-without-wi-fi.
[10] "Coronavirus: When the state shifted to e-learning, this rural school superintendent shifted to the copy machine." https://herald-review.com/news/state-and-regional/coronavirus-when-the-state-shifted-to-e-learning-this-rural-school-superintendent-shifted-to-the/article_ec0ac0c1-de70-5da8-8820-e4f04a30f65f.html.
[11] "Fixed broadband deployment," July 2020. https://broadbandmap.fcc.gov.
[12] "The Covid-19 pandemic shows the virtues of net neutrality." https://www.wired.com/story/covid-19-pandemic-shows-virtues-net-neutrality.
[13] "Go ahead, stream all you want. the internet is fine—for now." https://www.wired.com/story/stream-all-want-internet-fine-now.
[14] "Forced online by virus, China's schools run into censorship." https://apnews.com/cbde0ac8f6b52a37206a6f374e1f0398.
[15] "Government tracking how people move around in coronavirus pandemic." https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202.
[16] "Privacy-preserving contact tracing," April 2020. https://www.apple.com/covid19/contacttracing.
[17] "Singapore government launches new app for contact tracing to combat spread of covid-19." https://www.mobihealthnews.com/news/asia-pacific/singapore-government-launches-new-app-contact-tracing-combat-spread-covid-19.
[18] "Three u. professors awarded nsf grants to study covid-19," 2020. https://www.dailyprincetonian.com/article/2020/04/nsf-grant-covid19.
[19] "Study: Contact tracing slowed covid-19 spread in china." https://www.cidrap.umn.edu/news-perspective/2020/04/study-contact-tracing-slowed-covid-19-spread-china.
[20] "Coronavirus: Moscow rolls out patient-tracking app." https://www.bbc.com/news/technology-52121264.
[21] "Israel's coronavirus surveillance is an example for others - of what not to do." https://privacyinternational.org/long-read/3747/israels-coronavirus-surveillance-example-others-what-not-do.
[22] "Ahead of the curve: South korea's evolving strategy to prevent a coronavirus resurgence." https://www.reuters.com/article/us-health-coronavirus-southkorea-respons/ahead-of-the-curve-south-koreas-evolving-strategy-to-prevent-a-coronavirus-resurgence-idUSKCN21X0MO.
[23] "Yelp: Local economic impact report." https://www.yelpeconomicaverage.com/yelp-coronavirus-economic-impact-report.
[24] "Covid-19 mobility reports." https://www.google.com/covid19/mobility/.
[25] "Smartphone data reveal which americans are social distancing (and not)." https://www.washingtonpost.com/technology/2020/03/24/social-distancing-maps-cellphone-location.
[26] "Strava fitness app can reveal military sites, analysts say." https://www.nytimes.com/2018/01/29/world/middleeast/strava-heat-map.html.
[27] "Open-access publishing and the coronavirus." https://www.insidehighered.com/news/2020/05/15/coronavirus-may-be-encouraging-publishers-pursue-open-access.
[28] "Open access to ACM digital library during coronavirus pandemic." https://www.acm.org/articles/bulletins/2020/march/dl-access-during-covid-19.
[29] C. Pancake, "Twitter." https://twitter.com/pancakeACM/status/1278447589646635019.
[30] "Move fast and roll your own crypto - a quick look at the confidentiality of zoom meetings." https://citizenlab.ca/2020/04/move-fast-roll-your-own-crypto-a-quick-look-at-the-confidentiality-of-zoom-meetings/.

[31] "Zoom end-to-end encryption whitepaper." https://github.com/zoom/zoom-e2e-whitepaper/.
[32] National Academies of Sciences, Engineering, and Medicine, *Securing the Vote: Protecting American Democracy.* Washington, DC: The National Academies Press, 2018.
[33] "Some states have embraced online voting. it's a huge risk.." https://www.politico.com/news/2020/06/08/online-voting-304013.
[34] "Researchers say online voting tech used in 5 states is fatally flawed." https://arstechnica.com/tech-policy/2020/06/researchers-say-online-voting-tech-used-in-5-states-is-fatally-flawed/.
[35] "UK internet voting comes under attack," *Network Security*, vol. 2007, no. 5, pp. 1 – 20, 2007.
[36] "Online voting is impossible to secure. so why are some governments using it?." https://www.csoonline.com/article/3269297/online-voting-is-impossible-to-secure-so-why-are-some-governments-using-it.html.
[37] Computer Science and Telecommunications Board, "The Internet under crisis conditions: Learning from September 11," 2003. National Research Council.
[38] J. Chan, "Taiwan earthquake triggers a "digital tsunami" in Asia." https://www.wsws.org/en/articles/2007/01/taiw-j09.htmls.
[39] E. Aben, "RIPE Atlas: Hurricane Sandy and how the internet routes around damage." https://labs.ripe.net/Members/emileaben/ripe-atlas-hurricane-sandy-global-effects.
[40] J. Borland, "Analyzing the internet collapse." https://www.technologyreview.com/2008/02/05/222155/analyzing-the-internet-collapse/.
[41] *CSX Tunnel Fire/USFA-TR-140 [July 2001].* Federal Emergency Management Agency, Jul 2001.
[42] "Internet infrastructure: Dhs faces challenges in developing a joint public/private recovery plan." https://www.govinfo.gov/content/pkg/GAOREPORTS-GAO-06-672/html/GAOREPORTS-GAO-06-672.htm.
[43] R. Durairajan, C. Barford, and P. Barford, "Lights out: Climate change risk to internet infrastructure," in *Applied Networking Research Workshop*, (New York, NY, USA), p. 9–15, 2018.
[44] G. Wolfsfeld, E. Segev, and T. Sheafer, "Social media and the Arab spring: Politics comes first," *The International Journal of Press/Politics*, vol. 18, no. 2, pp. 115–137, 2013.
[45] "Censorship and social activism in the Middle East and North Africa censorship." https://www.secdev-foundation.org/wp-content/uploads/2016/07/MENA.pdf.
[46] R. Hiran, N. Carlsson, and P. Gill, "Characterizing large-scale routing anomalies: A case study of the China Telecom incident," in *Passive and Active Measurement*, 2013.
[47] "YouTube hijacking: A RIPE NCC RIS case study," March 2008. https://www.ripe.net/publications/news/industry-developments/youtube-hijacking-a-ripe-ncc-ris-case-study.