



5th USENIX Workshop on Free and Open Communications on the Internet (FOCI '15)

Sponsored by USENIX, the Advanced Computing Systems Association

August 10, 2015, Washington, D.C.

FOCI '15 will be co-located with the 24th USENIX Security Symposium (USENIX Security '15) and take place on Monday, August 10, 2015.

Important Dates

- Submissions due: **Tuesday, May 19, 2015, 8:59 p.m. PDT**
- Notification to authors: **Tuesday, June 23, 2015**
- Final papers due: **Friday, July 24, 2015**

Workshop Organizers

Program Co-Chairs

Masashi Crete-Nishihata, *Citizen Lab, University of Toronto*
 Phillipa Gill, *Stony Brook University*

Program Committee

Ryan Budish, *Berkman Center for Internet and Society*
 Jed Crandall, *University of New Mexico*
 Roger Dingledine, *Tor Project*
 Roya Ensafi, *Princeton University*
 Nick Feamster, *Princeton University*
 Amir Houmansadr, *University of Massachusetts Amherst*
 Christopher Parsons, *Citizen Lab, University of Toronto*
 Vern Paxson, *University of California, Berkeley, and International Computer Science Institute (ICSI)*
 Jon Penney, *Oxford Internet Institute, Berkman Centre for Internet, and Citizen Lab*
 David Robinson, *Robinson + Yu*
 Nick Weaver, *University of California, Berkeley, and International Computer Science Institute (ICSI)*
 Meredith Whittaker, *Google Research*
 Joss Wright, *University of Oxford*

Steering Committee

Jed Crandall, *University of New Mexico*
 Roger Dingledine, *The Tor Project*
 Nick Feamster, *Georgia Institute of Technology*
 Casey Henderson, *The USENIX Association*
 Wenke Lee, *Georgia Institute of Technology*
 Kurt Opsahl, *Electronic Frontier Foundation*
 Vern Paxson, *University of California, Berkeley, and International Computer Science Institute (ICSI)*
 Joss Wright, *University of Oxford*

Overview

The 5th USENIX Workshop on Free and Open Communications on the Internet (FOCI '15), to be held on August 10, 2015, seeks to bring together researchers and practitioners working on means to study, detect, or circumvent practices that inhibit free and open communication on the Internet.

Internet communications drive political and social change around the world. Governments and other actors seek to control, monitor, manipulate, and block Internet communications for a variety of reasons, ranging from extending copyright law to suppressing free speech and assembly. Methods for controlling what content people post and view online are also multifarious. Whether it's traffic throttling by ISPs or man-in-the-middle attacks by countries seeking to identify those organizing protests, threats to free and open communications on the Internet raise a wide range of research challenges.

FOCI '15 invites submissions from technical as well as policy and social science-oriented research. Work that combines perspectives from multiple fields is especially encouraged.

We encourage submission of new, interesting work on a wide variety of topics of interest, including but not limited to the following areas:

Network Interference and Internet Censorship

- Capabilities and constraints of Internet filtering technologies
- Techniques for measuring the prevalence and operation of deployed national-level Internet censorship systems
- Studies and findings on real-world censorship or tampering from field deployments or other methods, such as the topics or content censored by states or the extent to which ISPs are degrading certain types of content or service
- Comparisons of existing tools that might be used to detect tampering, blocking, or violations of net neutrality
- Metrics and benchmarks for content tampering or performance degradation
- Detection, measuring, and analysis of the censorship of search results
- Ethical and legal issues surrounding measurements of network interference and Internet censorship

Surveillance

- Analysis of passive or targeted surveillance systems
- Techniques to counter passive or targeted surveillance or its effects

Circumvention

- Evaluation or analysis of existing anti-censorship systems
- Design of network protocols and topologies that resist tampering or blocking
- Capabilities of deep packet inspection (DPI) and robust mechanisms to circumvent DPI
- Usability in censorship-resistant systems

Policy

- Effects of information control on individuals, society, business, or political processes
- Analysis of policy processes behind censorship / surveillance regimes
- Analysis of the economic impact of censorship
- The role of private corporations in spreading or enabling surveillance/censorship

FOCI favors interesting and new ideas and early results. We envision that work presented at FOCI will ultimately lead to more mature publications at relevant, high-quality conferences. Papers will be selected primarily based on originality, significance, and technical merit, with additional consideration given to their potential to foster productive discussion at the workshop.

Submission Instructions

Submitted papers must be no longer than eight 8.5" x 11" pages, based on the standard USENIX format. References do not count towards the page limit. Specifically, your paper should be typeset in two column format in 10-point type on 12-point (single-spaced) leading, with a text block no more than 6.5" wide by 9" deep. All papers must be submitted via the Web submissions form, which is available on the FOCI '15 Call for Papers Web site at www.usenix.org/foci15/cfp.

Unlike previous years, this year's FOCI submission process will be single-blind. Authors should include their names on their submission and do not need to blind references. Contact the program co-chairs at foci15chairs@usenix.org if you have any questions.

Papers that do not comply with the submission requirements may be rejected without review. All accepted papers will be available online to registered attendees before the workshop. If your paper should not be published prior to the event, please notify production@usenix.org. The papers will be available online to everyone beginning on the day of the workshop, August 10, 2015

Simultaneous submission of the same work to multiple venues, submission of previously published work, or plagiarism constitutes dishonesty or fraud. USENIX, like other scientific and technical conferences and journals, prohibits these practices and may take action against authors who have committed them. See the USENIX Conference Submissions Policy at www.usenix.org/submissionspolicy for details. Note, however, that we expect that many papers accepted for FOCI '15 will eventually be extended as full papers suitable for presentation at future conferences.

Questions? Contact your program co-chairs, foci15chairs@usenix.org, or the USENIX office, submissionspolicy@usenix.org.

Papers accompanied by nondisclosure agreement forms will not be considered. Accepted submissions will be treated as confidential prior to publication on the USENIX FOCI '15 Web site; rejected submissions will be permanently treated as confidential.

