Laura Huey

University of Western Ontario, Canada. lhuey@uwo.ca

Welcome to the inaugural run of *Surveillance & Society*'s new debates/discussion section!

We have launched this new section in order to promote the exchange of ideas and discussion of relevant topics among readers. To that end, each year we will invite a group of discussants to contribute papers in a selected topic area to be published annually in the December issue. These papers are intended as means of stimulating readers to respond with their own thoughts, in the form of commentaries we will seek to publish in future issues within the year following.

To help us get started, we invited discussants from various fields, who kindly agreed to respond to one or more of three questions we posed to orient the discussion. This year's panel of invitees is:

danah boyd, *Microsoft Research*
Steven T. Margulis, *Grand Valley State University* and Gary T. Marx, *M.I.T.*
Judith Rauhofer, *University of Edinburgh*
Paul Rosenzweig, *Red Branch Consulting* and *George Washington University*
Micheal Vonn, *BC Civil Liberties Association*
Reg Whitaker, *York University* and the *University of Victoria*

Our focus for this year is "The Future of Privacy Online: Three Questions." Why the future of online privacy? Given that there has been much recent debate on the future of online privacy within academic and policy-making circles, as well as among members of the general public, we thought it would be an illuminating exercise for readers if we were to ask contributors from different fields, and with different perspectives, to share their views on what we see as three important questions. These questions are:

In relation to online privacy ...

- i) Where are we?
- ii) What should the future look like?
- iii) And what is the best means of acquiring that future?

We also asked participants to address their response by selecting one of three areas:

- social media,
- other forms of information technology, and
- national security.

We received six commentaries with six unique views on the questions posed. Three of our invited authors opted to tackle some of the thorny issues that arise in discussions of privacy and national security in the online context. Surveying the landscape of online privacy in the post 9/11 world, Micheal Vonn says those individuals and groups who support traditional notions of privacy are in “deep sh**” because of the speed at which privacy-piercing technologies proliferate, and the haste with which governments and other actors attempt to exploit them. However, Vonn is not ready to throw in the towel. Instead, she is issuing a rallying cry, one founded on the belief that privacy is not dead, it just needs a make-over: “we need a new model and understanding of privacy that gives this value its appropriate weight culturally, legally and constitutionally.” Reg Whitaker is also taking stock of the digital environment post-9/11 and similarly appears to not like what he sees: a series of Western governments that have enacted privacy invasive legislation, frequently with little or no consultation or justification for measures taken. Whitaker notes one interesting exception: Canada. Tracing the history of Canada’s efforts to pass legislation that would similarly provide security agencies with enhanced data-tapping and other online investigative powers in the face of substantial public opposition, what is revealed is—potentially—a model of resistance for other nations. Taking an entirely different tack, Paul Rosenzweig wants to solve what is often viewed as an intractable problem by policy-makers: the privacy-security zero sum game in which any move to increase or decrease online privacy or other freedoms is met with a commensurate increasing or decreasing of public security. For Rosenzweig, this zero sum game occurs because we treat privacy as an absolute rather than instrumental right. He suggests that we should move away from viewing privacy as being synonymous with anonymity and instead reconceive it as a limitation on consequence, paying greater attention to “the means/ends/consequence fit of any proposed dataveillance program.”

Focusing on information technology more generally, danah boyd also believes that it is time for a change in our approach to understanding privacy. For boyd, liberal democratic conceptions of privacy as an individual right do not work well within networked societies. In essence, she argues that to the extent that most of us do not “bowl alone” in the online world, we need to shift towards models of privacy that “position networks, groups, and communities at the center of our discussion.” Stephen Margulis and Gary Marx have also opted for an examination of information technology—in particular, they explore e-commerce in the U.S. and what social science research has to tell us about the treatment of privacy concerns online. Summing up this body of research, the legislative history of an assorted number of proposals in the U.S. Congress, various voluntary privacy-enhancing schemes and their limitations, these authors conclude that it is likely that the protection of consumers’ privacy will remain in the hands of the private sector and, in particular, those of consumers. Thus, their warning: “*caveat emptor*.” Judith Rauhofer is not satisfied with the *caveat emptor* approach. One reason for her dissatisfaction is that, as she notes, the current economic crisis too easily allows e-businesses to claim privacy-infringing data collection practises as economic necessity and thus trump lesser considerations, such as consumer privacy rights. As she puts it, “at a time of global recession, the economic imperative has therefore joined ‘national security’ as the public policy objective of choice to which individuals’ privacy is expected to take a backseat.” To help stop our current “race to the bottom,” she too is suggesting a shift in perspective: away from “the existing defensive discourse around data protection” toward a multi-pronged “positive agenda for privacy” that includes social normative, technological and public policy components.

Now that we have the ball rolling in the form of the thought-provoking contributions that follow, we invite interested readers to consider participating in the forum by responding to, elaborating on, or otherwise contributing their own thoughts and ideas on this topic. Responses should be in the form of a “comment” that addresses the content of a given piece and is thus of no more than 3-5 pages double-spaced in length. Please send your comments to the Debates Editor, Laura Huey (lhuey@uwo.ca). These will be reviewed by her upon submission, and she may seek revisions concerning any typos, spelling/grammar, unclear language or unsuitable content.