BUILDING AN INFRASTRUCTURE FOR THE FUTURE

*Yochai Benkler**

There are all sorts of reasons why we might care about the future of the law that regulates encryption technology, and in a sense the title of today's conference suggests a number of possible reasons.

Is this debate about e-commerce? Encryption enables confidentiality and authenticity, which we need in order to complete transactions. Is encryption important because without it e-commerce will not flourish? Well, that is one reason.

Is it because we are concerned about crime and the use of encryption to cover up crime? Is it a matter of law enforcement? Clearly, that is an issue for many who care about encryption regulation, as we will see in this morning's panel.

Is it because encryption regulation is a form of speech regulation and thus a First Amendment matter? That is another issue that makes our debate important for many, as Eben Moglen so vividly argues.

What I would like us to think about—and I think we will get differing perspectives on this issue from the participants in the panels—is that the encryption debate has arisen in a broader context. The debate highlights one instance of a general problem: law distributes control over the flow of information in an environment whose infrastructure for control has changed dramatically, and must be designed with concern for its effects on the distribution of control. Think about the shift from encoding religious texts in Latin scripts, which most people do not understand and cannot access, to presenting the texts printed in the vulgar tongue, so that many people can possess a bible and understand it. We are experiencing a similar shift in the distribution of control over access to information, based on a new mechanism of encoding and decoding, which is disseminated by a new technology for storing and distributing the information.

The encryption debate needs to be understood as a debate about what we do when our digitally networked environment recreates the ways in which we encode and decode information, and the ways in

* © Yochai Benkler. Associate Professor of Law, New York University School of Law. Non-exclusive license granted to *New York University Journal of Legislation and Public Policy* to publish in hard copy, on electronic databases or web pages.

which we share it or block access to it. Digitization radically changes the way we control the flow of information in our environment, but does so in two diametrically opposed directions. On the one hand, it opens information up—for search, for access, for processing—in a way that was never before possible. Walls and bureaus can no longer protect information, as they did when information was encoded and stored on ink and paper. That makes information much more obtainable and much harder to keep confidential. However, on the other hand, cheap processors and effective encryption algorithms also make it much harder to access information than if it were locked in a bureau that could be broken open (with or without a warrant depending on who does the breaking). Encryption, therefore, enables a confidentiality that was never before possible.

Similarly, not only can information be very widely distributed, but it can also be efficiently collected from a wide range of sources, and controlled in a centralized fashion as we generate information about ourselves through our lives in the digitally networked environment. This raises the questions: Who controls information about us? Does each person living her life control her own information? And is that a good thing or a bad thing? Is there government control over this information? Is there business control over this information?

Encryption regulation stands, in a sense, as Cerberus, protecting the entry to the netherworld, but no one quite knows—or at least we have deep disagreements about—which world is netherworld and which world is ours. Is the other side anarchy and ours order? Or is the other side statism and ours freedom? Is the other side pervasive surveillance? Or is the other side self-governance?

An increasingly large portion of our lives is conducted in the digitally networked environment. Control over the information that we generate in our day-to-day communications with each other, and in general in our behavior and our lives on the Net, will become increasingly important to the question of how we present ourselves to the world. Thus, how we control the technology which controls information flows among individuals, corporations, and governments will to a great extent determine how our society is structured—who will be able to know what about whom, and how they will be able to use that information and affect the behavior of the objects of their observation. I think that as we go to the panels and we hear the different perspectives and the different contexts in which concerns about encryption arise as discreet regulatory issues, it is important to relate back to these general questions of how decisions regarding whether and how to regulate encryption will affect who controls what information, who can gain access to what information, and who can force access to what information.