Software Freedom Law Center

Eben Moglen
+1-212-461-1901
moglen@softwarefreedom.org

Testimony of Eben Moglen

1995 Broadway, 17th Floor
New York, NY 10023-5882

tel +1-212-580-0800
fax +1-212-580-0898

www.softwarefreedom.org

December 2, 2010

US House of Representatives
Committee on Energy and Commerce
Subcommittee on Commerce, Trade & Consumer Protection

Mr. Chairman and Members of the Subcommittee,

Thank you for the invitation to appear today to help the committee address this very important subject.

"Social networking" offers immense economic, educational and personal opportunities for people everywhere. Rapid adoption of technologies for sharing information among socially connected but geographically dispersed groups is changing how we live, how we work, and how our children learn about the world. But social networking as we presently use it is technically arranged as "centralized" services, in which one party—let us call it "Facebook" for convenience—keeps all the data that everyone is sharing with everyone else in one big database. The service provider absolutely controls this database, which they can access however they like, regardless of the controls over third party access to the data, and which they can build profitable "data mining" activities atop.

This situation, in which one business controls all the shared data of hundreds of millions of people, is not a technical requirement, but rather a bad design decision grown out of control. The Internet and the World Wide Web, which are the technical infrastructures on which social network applications sit, does not require centralized control of shared data. All the technical features people like about social networking could be delivered to them without centralized data storage and the resulting privacy invasions.

Facebook and similar centralized social networking services like to talk about their "privacy settings." This is mere deception, a simple act of deliberate confusion. These "privacy settings" merely determine what one user can see of another user's private data. The grave, indeed fatal, design error in social networking services like Facebook isn't that Johnny can see Billy's data. It's that the service operator has uncontrolled access to *everybody's* data, regardless of the so-called "privacy settings."

Facebook holds and controls more data about the daily lives and social interactions of half a billion people than 20th-century totalitarian governments ever managed to collect about the people they surveilled. As viewers of a recent motion picture are aware, Facebook was not the result of careful, thoughtful development by technologists concerned with the ethical dimension of information technology. Instead, immature technology created by immature people has become popular, and valuable, despite its manifest defects. Because those defects are potentially profitable, giving the holder of social network databases unparalleled access to people's internal lives, unregulated commercial activity will not solve the problem of initial technological misdesign: commercial motives uncontrolled by regulation in the public interest will make the problem worse.

The nature of the technological redesign required to give people everywhere the ubiquitous benefits of social networking without the negative consequences of centralized for-profit spying is well-understood. Mr. Rafael Sofaer, from whom you have already heard, is one of the young technologists working to replace the poor design that yielded Facebook with designs that can serve individual needs without harming the public interest in maintenance of individual privacy. He and his colleagues in the Diaspora project, along with hundreds of other volunteers in the free software and open source movement who make great computer software to share, are already bringing into existence the second-generation social network architecture that offers sharing to everyone, without putting anybody in the middle, holding all the data for everybody else. Using a social network service like Face-

book means that every time you *access* anybody else's shared data, you're making a record about yourself. Facebook knows not only what everybody posts, but also what everybody reads. Users of systems like Diaspora, however, can be sure that only the parties actually sharing know who accesses their data: no one else knows whether Susie is checking Billy's page, and everything Billy shares he shares from a safe place under his own, not Mr. Zuckerberg's, control.

But regulation of social networking technology in the interest of privacy can't work by regulating technology. Government cannot determine what innovations *will* happen, let alone determine what *should* happen. Nor can agency rulemaking—which is a slow and complex process that powerful businesses can more easily influence than individuals—be counted upon to respond with speed and agility to market developments that harm the public interest.

Instead, Congress should look at privacy questions from the same regulatory perspective used to address the issue of environmental quality, when—under the Nixon Administration—the Federal Government began making serious attempts to improve the environmental health of the United States. We need a National Privacy Policy Act, like the National Environmental Policy Act, in which Congress declares the clear overall national goals to be pursued, and requires federal agencies to assess all their regulatory activities in light of those goals. As with environmental law, Congress needs to entrust a lead agency with the primary responsibility for bringing to bear technical as well as legal and political resources in that effort. The Federal Trade Commission is plainly suited to the role of lead agency on privacy, and its traditional mode of activity since 1915, namely the investigation and "prosecution" of complaints, is the appropriate regulatory style. The FTC can and does behave with the agility and perseverence necessary to obtain compliance with the public interest in complex and fast-changing marketplaces. Empowered by clear and specific Congressional declarations of national privacy policy, the Commission would be well positioned to use its traditional tools to protect the public interest.

Precise delineation of national privacy goals will require full public debate and careful Congressional consideration. As with environmental policy, businesses with bad records of deteriorating the public interest can be expected to demand inaction, rather than reinvigorated protection of the public. But poor technological design with profoundly unethical public consequences does not become sacrosanct once it makes a lot of money.

Thank you.