



June 6, 2016

Dear Massachusetts Senators and Representatives,

We, the undersigned technology experts, business leaders, and academics, urge the Massachusetts congressional delegation to oppose legislative efforts to weaken the digital security tools upon which millions of people and thousands of businesses in Massachusetts, the nation, and the world rely.

Congressional action to force technology companies to weaken digital security would put American businesses at a global disadvantage, threatening both consumer protections and the vibrancy of the Massachusetts economy, which relies uniquely on a thriving high tech industry.

Massachusetts enjoys the highest per capita high tech workforce nationwide. The industry group CompTIA estimates that one in ten Bay State workers is employed in the technology sector. These 286,000 tech jobs offer an average annual wage of \$121,000. The Massachusetts Technology Leadership Council, in turn, finds that tech industry business and employee spending sustains another 400,000 workers statewide, in fields ranging from low-wage restaurant work to high-priced consultancies.

Digital security is a requirement for both consumer safety and economic resilience. Every day, Americans and their businesses rely on strong encryption to safeguard banking transactions, health records, and even classified government information. Strong digital security shields people from potentially catastrophic identity theft, corporations from industrial spying, and health care, finance and legal professionals from harmful disclosures of privileged patient or client information.

Contrary to popular misconception, there is simply no way to create a “backdoor” into otherwise secure systems that can only be accessed by law enforcement. Systems either integrate strong security protocols or they don’t.

Maintaining secure code is extremely difficult for even the most advanced technology companies. Asking tech firms to maintain two separate stacks of code—one stack legitimate and as secure as possible, and the other deliberately insecure—puts an enormous burden on even the most advanced and well-resourced companies. Smaller tech startups likely won’t survive such a requirement, or will face the impossible prospect of asking their users to rely on insecure code.

Forcing technology companies to build law enforcement access into digital systems creates weaknesses that can be exploited by actors with nefarious intent. Law firms, banks, health care and other corporations that today rely on auto-updates and secure technology products to protect sensitive information would face heightened risks of industrial espionage and security breaches. If users cannot trust software updates from American companies, they may not install them, leaving their systems vulnerable to hacks.

The threat from such laws wouldn't be limited to the security of technology systems. Legislation to conscript private companies to intentionally weaken their security on behalf of law enforcement also threatens the ability of U.S. technology companies to compete in the global marketplace.

If U.S.-based corporations are forced to comply with government demands to hack their own users, business customers will look to other nations for secure products. The economic impact of the resulting hit to the United States technology industry would be profound, especially for the high-tech Massachusetts economy.

Strong digital security tools protect our nation's information economy. Digital security enables American technology companies to flourish in the global marketplace. Digital security protects American consumers, businesses, and jobs.

For these reasons, we respectfully ask that you reject proposals to weaken America's digital security.

Sincerely,

Hal Abelson, Professor, MIT

Colin Angle, CEO, iRobot

Yochai Benkler, Professor, Harvard

Joshua Boger, Executive Chairman, Alkeus Pharma

Sasha Constanza-Chock, Professor, MIT Center for Civic Media

Dr. Kate Crawford, MIT Visiting Professor, Center for Civic Media

Richard Ferrante, Principal, RDF Software Group

Deborah Hurley, Harvard University

Joichi Ito, Director, MIT Media Lab

Ronald Rivest, Institute Professor, MIT

Carol Rose, Executive Director, ACLU of Massachusetts

Paul Sagan, Executive in Residence, General Catalyst Partners

Bruce Schneier, Fellow, Kennedy School of Government, Harvard University

Chris Schoettle, President & COO, Enservio

Wendy Seltzer, Research Scientist, MIT

Gerald Jay Sussman, Panasonic Professor of Electrical Engineering, MIT

Latanya Sweeney, Professor, Harvard

Daniel J. Weitzner, Principal Research Scientist, MIT

Andy Yen, Co-Founder and CEO, ProtonMail

Ethan Zuckerman, Principal Research Scientist, MIT Media Lab, Director, MIT Center for Civic Media