

Summary: Government should promote and police verification as a core Internet wide service, and social media operators should be incentivized to support competition through interoperability.

The Honorable Amy Klobuchar
United States Senate
425 Dirksen Senate Building
Washington, DC 20510

January 12, 2024

Dear Senator Klobuchar,

As a co-founder of the UofM supercomputing center and Director of its networking group, I “pioneered” the Internet in Minnesota during the 1980s (see MRNet <https://tcjnet.com/mrnet/>). We dreamt of a global, distributed, level, and free means for information, collaboration, and debate.

As you know, a few large monopolies and some malicious individuals have pursued a course that is antithetical to our original, perhaps naive, vision. As I understand it, your efforts to rein-in social media, AI, etc. has not yet been successful. I believe addressing the subjective social problems of misinformation etc. will be a long step-by-step process of “whack a mole,” often against very powerful opposition.

I am writing to suggest that there are two innocuous purely technical steps, based on proven technology and methods that can be taken immediately if kept simple and “under the radar”. These will have broad and significant positive effect, and may be prerequisite to anything you do in law. Briefly:

1. Verification (a.k.a. Digital Identity/Digital Credentials/Notary/Watermarking/Authentication, etc.)

The Federal government should promote and police, together with the Internet Engineering Task Force (IETF), the World Wide Web Consortium (W3C), et al. the expansion of existing Internet-wide mechanisms such that when you get an email, read a tweet or post,

receive a chat, view a photo, or visit a website, you can know with a high degree of certainty it is unaltered, and the source is who they claim to be. By this I don't mean an internal product feature or service as offered by some social media operators, but an independent and Internet-wide distributed core service, monitored by government, with legal consequences for fraudulent use, that can be easily added to any application.

As an example, consider that e-commerce today would be impossible without verification/authentication services.

While not perfect, verification is an enabling part of techniques that can greatly stem the flood of malicious porn, spam, bots (AI and otherwise), financial scamming, identity theft, and misinformation. (I believe issues of Orwellian invasion of privacy can be managed through the use of various blind encryption techniques that guarantee anonymity.)

Further, verification may enable the development of a culture of credible sources, similar to the way certain print media, such as NYT, WaPo, The Times, and Le Monde, etc., have earned our trust in the past.

2. Interoperability

The Internet and Web were designed as a robust distributed system. Within this system a number of the largest players have worked to build "walled gardens," subverting the Web for business or political purposes, gleaning our personal information, blocking competition, and fomenting misinformation.

Recently several initiatives, in one case referred to as the "fediverse" (see: <https://w.wiki/8Rgh>), have begun to deploy distributed social media protocols which allow competing platforms to interoperate/interwork, much like email already does. Decentralizing/de-monopolizing social media is possible (regardless of what some vested interests might claim), and will help promote the development of a healthy, democratic, and multicultural/multinational social media

landscape. Such interoperability is very much in keeping with those core design principals that have made the Internet a success.

Implementation

The Internet was designed to facilitate rapid evolutionary technical change. The implementation of verification and interoperability enhancements standardized by the IETF and W3C need not be disruptive, and their use can be voluntary (i.e. coerced ;-).

It is widely accepted that one role of the federal government is the promotion of technical standards (e.g. NIST) for the benefit of the nation. While the federal government can not force adoption, it can eventually justify requiring these technologies for all its agencies, contractors, and grantees (e.g. universities), etc.

Action

Your office could help catalyze and fund a Minnesota (or national) task force within the context of engineering forums such as the IETF, W3C, et al. perhaps with oversight by the NAS, NSF and/or the Internet Society. With the help of such a task force engineers could accelerate the adoption of these technologies (the IETF motto is “rough consensus and running code”) in a way similar to the grass roots approach I used in creating MRNet in the 1980s. Eventually you could propose legislation to add “boiler plate” language to Federal funding.

Although I am retired, I would be glad to explain more, provide technical details and examples, and suggest a few well-regarded non-partisan individuals who might be willing to contribute to such an effort.

Sincerely,
Thomas Jacobson
www.tcjnet.com
thomas@tcjnet.com
Cell: 218 269 1198