1 Online social climate

In the next decade, will public discourse online become more or less shaped by bad actors, harassment, trolls, and an overall tone of griping, distrust, and disgust?

Online communication becomes MORE shaped by negative activities

Online communication becomes LESS shaped by negative activities

I expect no major change in the tone of online interaction

Please Elaborate on your response below.

Type your name at the start if you are willing to take credit for your response. We encourage you to also include your job title and workplace if you are willing as it adds context to your answer. If you do not type your name you will remain anonymous.

Please consider addressing these issues in your response: How do you expect social media and digital commentary will evolve in the coming decade? Do you think we will see a widespread demand for technological systems or solutions that encourage more-inclusive online interactions? What do you think will happen to free speech? What might be the consequences for anonymity and privacy?

* * *

M. E. Kabay, PhD, CISSP-ISSMP

Professor of Computer Information Systems

School of Business & Management

Norwich University / Northfield, VT

* As the global economy increases the number of people with modest disposable income, increasing numbers of people in developing countries around the world will use smartphones to access the Internet (or the restricted portions of the 'Net permitted by increasingly terrified dictatorships).

* We will see increasing participation in social networks, including increasing numbers of comments by new users.

* The widespread availability of anonymity and pseudonymity will encourage social disinhibition: without real-world consequences for intemperate remarks and trolls (attempts to provoke angry responses), the amount of negativity will increase.

* The numbers of new users will overwhelm the resources dedicated to monitoring and purging (some) social networks of abusive language; even today, networks such as Facebook are experiencing difficulty in taking down abusers.

* Censorship is already a major problem around the globe where frightened minorities continue to grasp at increasing levels of control to forestall revolution. Restriction of speech is growing even in privately-owned venues such as the popular social-media sites; the current approach is focused on removing abusive postings and blocking abusive members, but there is nothing to stop corporations from limiting speech in any way that fits their end-user license agreements (EULAs). EULAs are civil contracts; even where free speech is protected from GOVERNMENT interference, there is no such limitation for private firms.

* Perhaps we will see the development of social media sites with stringent requirements for traceable identity. These systems may have to demand evidence of real-world identity and impose strong (e.g., multifactor) authentication of identity. Even so, malefactors will continue to elude even the best of the attempts to enforce consequences for bad behavior.

2 Education, jobs, and skills

In the next ten years, do you think we will see the emergence of new educational and training programs that can successfully train large numbers of workers in the skills they will need to perform the jobs of the future?

Yes

No

Please elaborate on your response below.

Type your name at the start if you are willing to take credit for your response. We encourage you to also include your job title and workplace if you are willing as it adds context to your answer. If you do not type your name you will remain anonymous.

Please consider addressing these issues in your response: What are the most important skills needed to succeed in the workforce of the future? Which of these skills can be taught effectively via online systems –especially those that are self-directed – and other non-traditional settings? Which skills will be most difficult to teach at scale? Will employers be accepting of applicants who rely on these new types of credentialing systems, or will they be viewed as less-qualified than those who have attended traditional four-year and graduate programs?

* * *

* We already have the technology in place to reach a significant portion of the globe's population even in developing countries -- smartphones. Asynchronous online education at simple levels of awareness and training can support massive improvements in technical competence and in creativity.

* At a basic level, everyone needs to be able to learn new concepts, vocabulary and skills to continue contributing to a changing world -- changing demographically, culturally, and physically (think global warming and overpopulation).

* Clearly READING is one of the most important skills, and online courses can help people learn this essential skill.

* Similarly, increasing technical vocabularies is achievable using simple online training tools.

* Effective online examination of acquired skills will support the effort to improve individuals and organizations.

* The most difficult skills include critical thinking: evaluation of multiple sources of information, some of them contradictory, in the absence of a known correct result.

* The acceptance of online training and education will evolve as evidence accumulates of correlations between such processes and metrics rooted in real-world evaluations.

3 Impact of algorithms

Algorithms will continue to have increasing influence over the next decade, shaping people's work and personal lives and the ways they interact with information, institutions (banks, health care providers, retailers, governments, education, media and entertainment) and each other. The hope is that algorithms will help people quickly and fairly execute tasks and get the information, products, and services they want. The fear is that algorithms can purposely or inadvertently create discrimination, enable social engineering and have other harmful societal impacts.

Will the net overall effect of algorithms be positive for individuals and society or negative for individuals and society?

Positives outweigh negatives

Negatives outweigh positives

The overall impact will be about 50-50

Please elaborate on your response below.

Type your name at the start if you are willing to take credit for your response. We encourage you to also include your job title and workplace if you are willing as it adds context to your answer. If you do not type your name you will remain anonymous.

Please consider addressing these issues in your response: What are the main positive changes you foresee? What are the main negative ones? What dimensions of life will be most affected – health care, consumer choice, the dissemination of news, educational opportunities, others? How will the expanding collection and analysis of data and the resulting applications of this information impact people's lives? What kinds of predictive modeling will make life more convenient for citizens? What kinds of discrimination might occur? What kind of oversight mechanisms might be used to assess the impact of algorithms?

* * *

* On the positive side, better algorithms for adapting output to _specific_ users' needs / values / priorities may indeed be helpful in speeding up and refining information flow appropriate for specific conditions.

* However, if the algorithms use pooled data and generalized computations of probabilities, the result may be a suppression of results for specific needs. We may be heading for lowest-common-denominator information flows.

* Another issue is the possibility of increasingly isolated information bubbles or echo chambers. If the algorithms directing news flow suppress contradictory information -- information that challenges the assumptions and values of individuals -- we may see increasing extremes of separation in world-views among rapidly diverging subpopulations.

* Warning bells should sound when individualized or group information bubbles generated by the selective algorithms diverge from some definition of reality. Supervisory algorithms should monitor assertions or information flows that deviate from observable reality and documentary evidence; the question remains, however, of whose reality will dominate. A dictatorship like that in Orwell's _1984_ would LOVE to have control over the algorithms selecting information for the public or for subsectors of the public. If information is power, then information control is supreme power.

4 Trust and the global impact of technology

Billions of people use cell phones and the internet now and hundreds of millions more are expected to come online in the next decade. At the same time, more than half of those who use the internet and cell phones still do not use that connectivity for shopping, banking, other important transactions and key social interactions. As more people move online globally both opportunities and threats grow.

Will people's trust in their online interactions, their work, shopping, social connections, pursuit of knowledge and other activities, be strengthened or diminished over the next 10 years?

Trust will be STRENGTHENED

Trust will be DIMINISHED

Trust will stay about the same

Please elaborate on your response below.

Type your name at the start if you are willing to take credit for your response. We encourage you to also include your job title and workplace if you are willing as it adds context to your answer. If you do not type your name you will remain anonymous.

Please consider addressing these issues in your response. Which areas of life might experience the greatest impact? Economic activity? Health care? Education? Political and civic life? Cultural life? Will the impacts be mostly positive or negative? What role might the spread of blockchain systems play?

* * *

* I think trust will increase simply because familiarity consistently increases even irrational trust. Risk analysis is not a strong point among human beings; a simple illustration is that many people fear death and injury from terrorist attacks far more than from domestic nutcases armed with automatic weapons, drunk drivers, and even ordinary car accidents. Reality has little influence over emotion.

* All of the areas named above are likely to be affected by the growing population of smartphone-equipped users, especially in developing countries. In East Africa, for example, we have already see major effects on economic justice simply because inland farmers have been able to find out how much their crops are being sold for in coastal cities. The tool for this information exchange? Mobile phones -- not even smart phones.

* Again, in East Africa and elsewhere, impoverished, cash-deprived rural family members have finally been able to benefit from the income of their diaspora simply through text messages facilitating money transfers -- quite separately from the official banking systems. This kind of disintermediation can be highly positive.

* Disintermediation (removing absolute control of centralized power centers) over information flows threatens established dictatorships; they will retaliate to suppress independent information flows. We have already seen several examples in which such governments have interrupted Internet access for their own citizens in what they perceive as emergencies; the PRC routinely does so using the so-called Great Firewall of China for controlling external information inputs.

* On the positive side, remote interactions for creative work have resulted in such brilliant innovations as virtual choirs (look up the work of Eric Whitacre for stunning examples). Augmented reality can include artistic efforts in addition to chasing imaginary pets as in Pokemon Go.

* See my course materials for Politics of Cyberspace for more material on these questions: http://www.mekabay.com/courses/academic/norwich/cs407/index.htm

* As for blockchain systems, these cryptographic signatures may help decrease anonymity, but they won't stop pseudonymity.

5 IoT

As billions more everyday objects are connected in the Internet of Things they are sending and receiving data that enhances local, national and global systems as well as individuals' lives. But such connectedness also creates exploitable vulnerabilities.

As automobiles, medical devices, smart TVs, manufacturing equipment and other tools and infrastructure are networked, is it likely that attacks, hacks, or ransomware concerns in the next decade will cause significant numbers of people to decide to disconnect, or will the trend towards greater connectivity of objects and people continue unabated?

Most people will move more deeply into connected life

Significant numbers will disconnect

Please elaborate on your response below.

Type your name at the start if you are willing to take credit for your response. We encourage you to also include your job title and workplace if you are willing as it adds context to your answer. If you do not type your name you will remain anonymous.

Please consider addressing these issues in your response: What is the most likely kind of physical or human damage that will occur when things are networked? How might governments and technologists respond to make things more secure and safe? Is it possible to network physical objects in such a way that they will generally remain safe for the vast majority most of the time?

* * *

* The Internet of Things (IoT) will result in even greater numbers of systems compromised by criminals to create ever-larger botnets (networks of "zombie" computers responding to instructions from "master" systems). Botnets are used for generating spam (unsolicited commercial email), especially for fraud. Use search string < refrigerator used for botnet > for examples.

* Distribution of malware such as ransomware is also facilitated by botnets. Botnets are also used for distributed denial-of-service (DDoS) attacks, in which targets are flooded with overwhelming traffic that can slow response time or even crash the targets.

* Some of the IoT includes controllers for critical infrastructure. The Stuxnet attack on Siemens centrifuges in Iran and other countries demonstrated the long-standing view of information warfare specialists that unprotected or underprotected supervisory control and data acquisition (SCADA) systems could be subverted to cause significant real-world damage, not just effects on information alone. Medical IoT devices are particularly significant when considering possible damage to people; so are connected automobiles, which have become computers with wheels. There are already many examples of how cars can be hacked at a distance; use the search string < car hacked crash > for reports.

* The fundamental issue is that security is an afterthought for much of the IoT; the manufacturers bear few consequences for misuse of their poorly engineered systems, so some managers elect to shift costs away from their development process and simply let consumers bear the brunt of the damages. The calculation is that they can pay less in fines than for better security. The notorious Ford Pinto exploding gasoline tanks is the classic example of this cost-shifting approach.

* There is NO REASON that IoT security cannot be improved; however, under the current economic system is largely free from independent regulation. When IoT devices are subject to the same stringent requirements that pharmaceuticals must meet, we will see some reduction of risk.