Fields of Electronics, Information, and Communication

Achievement

Contribution to leading research for building an ethical digital society, including differential privacy and fairness

Prof. Cynthia Dwork (USA)
Born: June 27, 1958 (Age: 67)
Professor of Computer Science, Harvard University

Increased risk in exchange for a convenient digital society

Society has been rapidly digitalized through technological innovations such as the Internet, AI, and big data, and online interactions are becoming an increasingly large part of economic activity and daily life. The convenience and efficiency of digital life are built upon a vast amount of data and the analysis of that data. Data is collected everywhere, and because it contains personal and confidential information within that is accessible both directly or indirectly, there are growing concerns about that information leaking to others or being used for surveillance. (See Figure 1.)

In addition, ethical and social issues are becoming increasingly serious as operations conducted to extract usable information from the reams of data available have led to discriminatory judgements being made by AI systems and to the algorithmic control of markets. Of particular concern are the strains on our political system and the capitalist economy spurred on by privacy violations and the erosion of the public nature of cyberspace, the benefits of which should be enjoyed by society as a whole rather than being monopolized by a few select companies and countries. Recent innovations in technologies such as generative AI have only exacerbated these problems.

Amending the inequitable distribution of information and lack of ethical responsibilities and ensuring social fairness are just some of the challenges faced by digital society that cannot be resolved easily using traditional legal frameworks and ethical standards.

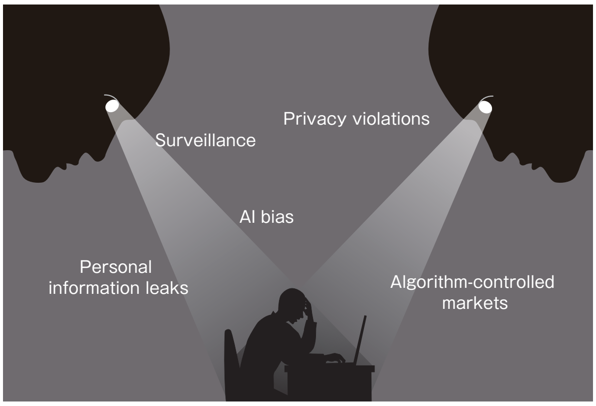


Figure 1: Concerns in a digital society

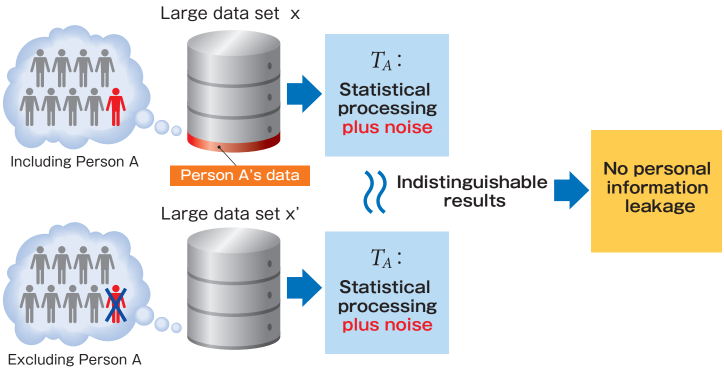
The public may be unknowingly subjected to AI and government manipulation, surveillance, and discrimination in cyberspace.

Differential Privacy – Evaluating personal information leaks

Prof. Dwork pioneered an entirely new academic field through the development of a mathematically rigorous theoretical framework for addressing ethical issues that arise in a digital society. Her 2006 proposal on “differential privacy” effected a particularly profound transformation in the way that personal information could be protected in the era of big data.

Differential privacy is a mathematical formulation guaranteeing that personal information within a set of data will not be revealed during analysis through presenting it in a way that it remains unchanged whether the data on a specific individual is included or not. (See Figure 2.) More importantly, it allows for the risk of personal information leaks to be evaluated mathematically before the public release of statistical data.

Furthermore, it has been shown that the intentional addition of a moderate amount of noise to the results of a statistical analysis can maintain its usefulness, and it can simultaneously ensure a result meets the desired standards for privacy protection, which has led to the use of this technique in various technologies and other products. Differential privacy has allowed companies and governments to obtain statistical information essential to the running of society


Large data set x
Including Person A
Person A's data
T_A:
Statistical processing plus noise
≈ Indistinguishable results
No personal information leakage
Large data set x'
Excluding Person A
T_A:
Statistical processing plus noise

Mathematical basis for protecting personal privacy during big data analysis

This equation shows that the absolute value of the natural logarithm of the ratio of probabilities that the statistical algorithm TA (including noise addition) will output the same result for two data sets x and x’ will be below a threshold ε. The lower the value of ε, the stronger the level of privacy protection becomes.

$$\left|\ln\left(\frac{\Pr[T_A(x)=t]}{\Pr[T_A(x')=t]}\right)\right| \leq \epsilon.$$

Figure 2: Protecting personal information through “Differential Privacy”

If the results of statistical analysis of large data sets cannot be distinguished from each other when the content of x and x’ differ only by the inclusion or exclusion of a single individual’ s data, personal information about that individual cannot be extracted. In other words, the individual’ s personal information would be therefore protected. Based on this idea, the amount of additional “noise” needed to prevent the leakage of personal information during statistical analysis can be computed mathematically.

while protecting user privacy, and it has been adopted for use in various services offered by major global IT corporations such as Apple, Google, Meta, Microsoft and NTT Docomo, and it was also used during the 2020 US Census.

Adopting the Proof of Work concept in cryptocurrency management

In 1992, Prof. Dwork had already predicted that the world would face a flood of spam email in the future, and gained attention for her proposal that a computational cost be implemented as a preventative mechanism. Her idea was that casual operations could be prevented by imposing a set amount of computational work and thereby incurring an economic cost when sending emails, creating transaction records, or performing other tasks. (See Figure 3.) This concept later came to be widely-known as "Proof of Work (PoW)," and it is used in the blockchain technology used for cryptocurrency systems, which first appeared in 2009. This demonstrated that reliable financial transactions are possible without a bank or other central administrator so long as the parties involved share a ledger of transactions made. In this way, an entirely new and egalitarian information sharing system was created.

Towards a secure and equitable digital society

In 2011, out of concern regarding the possibility that AI could make judgements based on societally inappropriate attributes such as race, gender, and age, Prof. Dwork began working on an algorithmic framework that would mathematically define and guarantee fairness called "Fairness through Awareness." Prior to this, she built a framework that could more rigorously guarantee the security of encrypted communications called "Non-Malleable Security".

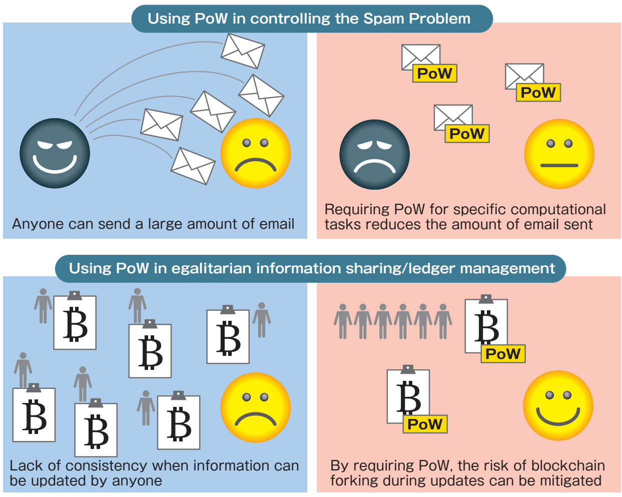
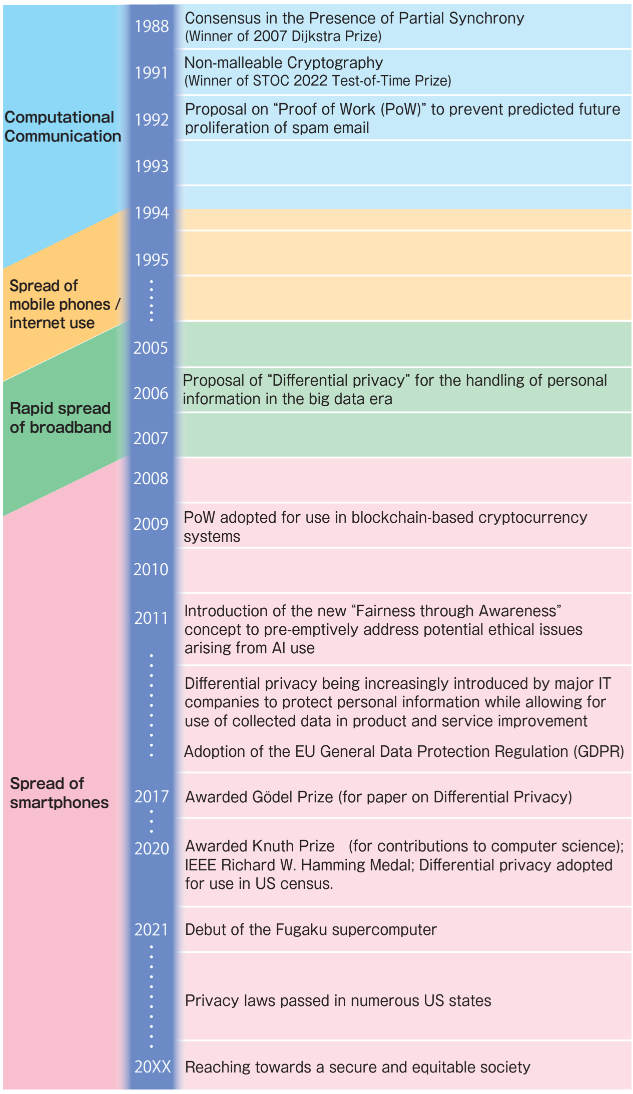

Using PoW in controlling the Spam Problem
PoW
PoW
PoW
Anyone can send a large amount of email
Requiring PoW for specific computational tasks reduces the amount of email sent
Using PoW in egalitarian information sharing/ledger management
PoW
PoW
Lack of consistency when information can be updated by anyone
By requiring PoW, the risk of blockchain forking during updates can be mitigated

Figure 3: The role of Proof of Work (PoW)

Casual operations, whether malicious or not, can be prevented by requiring a set amount of computational work to be completed whenever emails are sent (top) or transactional records are created (bottom). This maintains order in a digital society.

These research projects spearheaded the exploration of the social and ethical risks underlying online economic activity and algorithm use that has grown with the continued development of information technologies, and offered a theoretical mathematics-based solution that could be harnessed before that growth could have a severely negative impact on society. It was not merely an abstract proposal, but is in fact already in wide use as the theoretical core that maintains the reliability of global information infrastructure and economic systems, all while continuing to protect the privacy and security of individual citizens. (See Figure 4.)

Prof. Cynthia Dwork is engaged in a wide range of collaborative research projects truly beneficial to society, and through that work, she has had a hand in the education of many talented individuals. Alongside these researchers, she will surely continue to be a driving force in protecting order in our increasingly complex digital society.


Computational Communication
Spread of mobile phones / internet use
Rapid spread of broadband
Spread of smartphones

1988	Consensus in the Presence of Partial Synchrony (Winner of 2007 Dijkstra Prize)
1991	Non-malleable Cryptography (Winner of STOC 2022 Test-of-Time Prize)
1992	Proposal on "Proof of Work (PoW)" to prevent predicted future proliferation of spam email
1993	
1994	
1995	
⋮	
2005	
2006	Proposal of "Differential privacy" for the handling of personal information in the big data era
2007	
2008	
2009	PoW adopted for use in blockchain-based cryptocurrency systems
2010	
2011	Introduction of the new "Fairness through Awareness" concept to pre-emptively address potential ethical issues arising from AI use
⋮	Differential privacy being increasingly introduced by major IT companies to protect personal information while allowing for use of collected data in product and service improvement
	Adoption of the EU General Data Protection Regulation (GDPR)
2017	Awarded Gödel Prize (for paper on Differential Privacy)
⋮	
2020	Awarded Knuth Prize (for contributions to computer science); IEEE Richard W. Hamming Medal; Differential privacy adopted for use in US census.
2021	Debut of the Fugaku supercomputer
⋮	Privacy laws passed in numerous US states
20XX	Reaching towards a secure and equitable society

Figure 4: The development of digital society and Professor Dwork's achievements

As digital society began to take form at the beginning of the 1990s, Prof. Dwork foresaw the ethical issues that could arise in the near future, and built a theoretical foundation to prevent such issues through rigorous mathematical models. She is currently working on ethical issues arising from the emergence of AI society.