1. Introduction

June 17, 1991

Jim Warren, Conference Chair

This concerns our future — our near future; ten years or less. And a long time thereafter.

For we are at a crossroads — as individuals, organizations and governments increasingly depend upon computerized information and digital communications.

In many cases, a fax machine will soon be as useful as a mail carrier on horseback, and paper files will be as practical as clay tablets. Consider only the last decade’s changes in personal communications with phone machines and voice-mail, personal banking with automated teller machines, writing with word processors, community newsletters with desktop publishing and mailed correspondence with fax machines.

Customs, policies, regulations and statutes governing this new environment will be created. The question is: Who will create them and what will they be?

ABOUT FREEDOM

How do we protect “freedom of speech” — when the fingers are the tongue speaking to the mind through the eye, in a room that is global in size? (Paraphrasing Dave Hughes’ analogy that appears later in this book.)

How can we guarantee “the right of the people peaceably to assemble” — when Hyde Park is in a village called Earth and the soapbox is a notebook computer with a modem?

How will we protect freedom of “the press” — when the press is a personal computer in someone’s home? Or when a publisher needs only a terminal, and news is delivered in milliseconds? When unfettered commentary circulates internationally — and content, tone and volume are unrestricted by economics, advertisers, broadcast licenses or national boundaries?

How do we “petition the government for a redress of grievances” as informed citizen action — when information is computerized and access is digital? Especially when the libraries are government computers and research is government-funded?

How will we ensure that “the right of the people to keep and bear arms, shall not be infringed” — when the most potent weapon is information and its access?

How can we remain secure in our “persons, houses, papers and effects, against unreasonable searches and seizures” — when paper is digital and mail is electronic? When our most valuable effects are personal data and confidential information, and computers are our vaults? How do investigators search a suspect’s electronic mail when it is commingled with mail of others in privately-owned electronic post offices? How is a suspect wiretapped, when their comments are interleaved with those of hundreds of thousands of non-suspects over international networks?

How can we avoid the automated monitoring (incidental or intentional) that is a trivial-to-do byproduct of computerized information — surveillance of finances, lifestyles, purchases, correspondence, personal views, association, political expression? How much misbehavior or “crime” could be discovered in the process of unrestricted monitoring?

How can thousands of innocent parties remain unharmed when a computer they share may contain evidence of a crime — and the accused has the right to “be confronted with the witnesses [and evidence] against him”? How can someone accused of a computer crime “enjoy the right to a speedy and public trial by an impartial jury of the State and district wherein the crime shall have been committed” — when there are less than a hundred sworn investigators and perhaps a dozen prosecutors, nationwide, who are technically competent to investigate and prosecute? Where is crime committed when state and national borders are crossed at the touch of a key?

As we protect these freedoms that are fundamental to a free society, how do we also assure that responsibility accompanies their exercise?

ABOUT PRIVACY

How do we protect personal privacy against degradation in that small town named Earth — when the neighborhood gossip uses a computer and the backyard fence is the global net? And where do we move when we want to make a “fresh start”? (As noted by Janlori Goldman, later in this book.)

When we share personal information with one person, should they freely computerize it for their own use? Share it with others? Exchange it with others? Sell it? Without our permission? Without our knowledge? Without our knowing its uses?
Is our name or other personal information “property”? If so, who owns it? How should it be protected? What’s the difference when personal information is held in paper form versus in machine form by an individual, versus in machine form by a small business, versus by a large “impersonal” corporation?

What about accuracy of personal data? Who has what responsibilities regarding such accuracy? In the case of inaccurate personal information, how can responsibility and value be determined when multiple parties are involved in originating and utilizing such information?

When we provide information that is computerized for one purpose, should it be used for other purposes? By government? By community organizations? Religious groups? The private sector?

Should our voter registration information be public? Should it be shared with political advocates seeking our vote? Should it be used for jury selection?

Should we have driver’s licenses like credit-cards with a magstripe on the back for use by traffic officers — and retail merchants with card-readers? Should our driving records be shared with insurance companies? Should automobile registration information be shared with car dealers? To recall defective vehicles for warranty repair?

Should we be able to identify a caller’s phone number when they “enter our home” through our telephone? Should they be prohibited from intruding without identifying themselves? Or, do we wish to be anonymous when we call others? Should companies be able to identify our number when we order by phone — or just make a query? Should time-sharing computers be able to identify the phone number of modems calling them for access — for billing and authentication?

Should patients be able to see their medical records? Psychiatric records? With what likely impact on physicians’ candor in essential treatment records? Should parents have access to student academic records? Counseling records? Discipline records? Should students have access to their own records? With what impact on teachers’ candid cooperation for students’ benefit?

Should personal information be used to “profile” probable behavior? For security risks, tax collection, government benefits, job applicants, credit risks, renters and rental owners? For finely honed advertisements — selling products, services, religion and politics?

Should our lifestyles, families and buying habits be profiled? Should direct-marketing solicitors use such information to contact only those who appear likely to want their products, or continue what they now do with its costly and irritating “junk-mail” consequences?

How do we balance the “right to know” — and sometimes the need to know — with robust protection of personal privacy? What responsibilities accompany protection of privacy?

ABOUT THIS BOOK

These are a few of the questions that were addressed in the First Conference on Computers, Freedom & Privacy. To our knowledge, this was the first time that experts and advocates representing this much diversity gathered to exchange perspectives — addressing the complex issues, problems and hopes that commingle at the intersection of computers, freedom and privacy.

This book is the published record of their discussions.

ABOUT YOU

Their uniform conclusion: *If the fundamental freedoms and personal privacy that are the foundation of any free people are to be protected, it is essential that citizens become informed and actively participate in shaping the impacts and great potential of the Information Age.*