A PRIVACY PRIMER FOR POLICY MAKERS

Written Testimony of

Jerry Kang

Acting Professor, UCLA School of Law

Before the Federal Trade Commission At Hearings on the

FTC's Consumer Protection Role in the Emerging

High-Tech, Global Marketplace

January 23, 1996

Introduction

{1}As we sit here, today, we are being silently inundated with waves of information. Consider just a sample of the data flowing about us: television and radio broadcasts, satellite transmissions, cellular communications, bits of information flying at the speed of light down fiber optic channels coursing like veins beneath the city's streets. This is what the National Information Infrastructure ("NII") is all about.

{2}My interest is in a particular substream of information moving through the NII: personal information. I am interested in such information because it implicates the right of information privacy. In this testimony, I present a brief primer for policy makers charged with the responsibility of managing this important right. The primer outlines a simplified six-step process of how to think clearly about privacy. This

methodology is based on two recent Executive Branch initiatives in the privacy area, both of which I have had the privilege of working on. The first is a set of privacy principles promulgated by the Information Infrastructure Task Force ("IITF") in June 1995. The second is a report on telecommunications privacy released by the National Telecommunications and Information Administration ("NTIA") of the Department of Commerce.

Step #1: Define fundamental terms.

{3}Although this threshold step sounds obvious, my experience in the privacy policy making arena suggests that much confusion is spawned by a lack of precise definitions. This should not be surprising since the very term "privacy" is a notorious chameleon, having different hues of meaning depending on the context.

{4}In American law, for example Fourth Amendment jurisprudence, "privacy" sometimes means the right to enjoy physical seclusion in particular sanctuaries, such as one's home. At other times it means the right to make fundamental, self-defining decisions, as in cases such as Roe v. Wade. But for our purposes, privacy should be understood more narrowly as information privacy: an individual's claim to control the terms under which personal information is acquired, used, and disclosed.

{5}Many related concepts, regrettably ill-defined, hover around the privacy debate. As an illustration, I pick one pair of often confused terms: privacy and

security. At least three salient differences exist between the concept of privacy and security. First, privacy is an ethical or legal claim asserted by an individual. By contrast, security is a descriptive state of data and data systems. Second, privacy concerns itself with only personal information, whereas security deals with all types of information. For instance, the secret recipe for Coca-Cola warrants tight security but does not implicate privacy because the recipe is not information about a person. Third, in crafting information policy, privacy should come prior to security. Proper security ensures that information flows only in the way it is supposed to, that it is available when necessary, that it is shielded from unauthorized access, that it is not improperly altered. But before adopting security measures, one must decide how personal information is "supposed to" flow in the first place. That requires thinking about privacy, about the rights and responsibilities that should govern the acquisition, disclosure, and use of personal information.

{6}Since many other concepts are commonly confused, it behooves policy makers always to have in hand a working glossary of relevant terms. My point here is not that a list of correct definitions exists somewhere out there in the pages of some academic journal. No such list exists. Even if such a list did exist, it would necessarily have to adapt to the specific policy context, since analysis, assumptions, and definitions interact dialectically with the process of real-world problem solving. But

adopting some set of clear definitions, roughly consistent with the extant academic and policy literature, is a crucial first step.

Step #2: Identify fundamental values.

{7}Policy makers must next understand the values and interests undergirding and undermining an individual's claim to control her personal information. Even a cursory review of the literature reveals myriad values that privacy supports. For instance, we seek control of sensitive information, such as medical data, since disclosure of such information in and of itself may cause embarrassment or a sense of violation. In other cases, we seek control of personal information for more instrumental purposes. Today, personal information in the wrong hands, could easily lead to financial fraud, theft of reputation, and theft of identity. For example, the reason why people keep their social security number confidential is not because they are particularly embarrassed about the combination of digits, but because that number may unlock numerous data banks holding sensitive information, such as one's checking account.

{8}There are many other values. Privacy might promote psychological well being. It might provide the deliberative space people need to exercise creativity and autonomy. It might support non-mainstream political activity and discourse, which pose risks to be sure, but also promote an effervescent, participatory democracy. It is no coincidence that totalitarian states, such as, the former Soviet Union, the present

North Korea, or the dystopia envisioned by George Orwell, all insist on discrediting privacy, as something sought only by criminals or deviants. Policy makers need to understand that privacy does more than hide shameful conduct. Indeed, one could make a rewarding study of the European attitude, which tends to characterize information privacy as a human right not to be peddled away against competing economic or institutional interests.

{9}With that said, a fair-minded policy maker must also understand the values and interests arguing against absolute privacy. Foremost are certain free expression values. Consider what would happen if Bill Clinton had sovereign control over every bit of personal information about him. Then the New York Times could not write an editorial using information about Bill Clinton without his approval. Such a prior restraint would not only violate current understandings of the First Amendment but also clash grossly with the polity's ideal of an open and accountable government.

{10}Other competing values sound in economic terms. The Direct Marketing Association, for example, contends that by acquiring and manipulating personal information, sellers can bring buyers more precisely what they want, when they want it. This seems to be a good thing. Other commentators claim that giving an individual too much control over personal information raises the costs of doing business and encourages fraud. For instance, a lender may want to know a potential borrower's history of financial trustworthiness. If in the name of privacy such information is

denied, then the lender may simply raise the costs of loans for all borrowers, trustworthy and not, to offset the additional financial risk caused by the lack of information.

Step #3: Understand the personal information flow.

{11}On the NII, information moves in novel ways, with novel speeds. In any particular information sector, policy makers must grasp how personal information is initially collected, subsequently transferred, disclosed, and used. Most importantly, they should focus on the initial collection of personal information because it is at this moment that privacy norms can be most easily enforced.

{12}Information is collected whenever an individual and an information collector interact in some manner. For example, when I present testimony to an audience at the Federal Trade Commission, I am the "individual", and each audience member is in some sense an "information collector." By interacting with me, the audience collects bits of personal information: that I am male, Asian American, a particular height, a particular age. In fact, any time an individual interacts with another person or sensory instrument, there is a potential for data collection.

{13}To provide another example more relevant for the FTC, consider what happens when a consumer buys a "widget" through the Internet using, say, a credit card. Obviously, the party selling the widget--the counterparty to the transaction--

collects information about the consumer. Typically, this includes name, address, shipping address, credit card number, and the fact that the consumer prefers a particular kind of widget.

{14}In addition to the counterparty, many other players may act as intermediaries who facilitate the transaction. There are electronic communication providers, such as Internet Service Providers, on-line services, and other telecommunications companies, that might collect transactional data related to that particular purchase. There are electronic payment providers, such as credit card or digital cash companies, that allow for exchange of funds through the new medium. With the need for authentication and security of communications, there might also be public-key certification authorities. All of these intermediaries, or transaction facilitators, may be collect telling transactional data in the silent background, in ways nearly invisible to the consumer.

{15}After understanding who is collecting personal information and how, policy makers must next identify how the information is being disclosed and used. If a company is disclosing a consumer's purchase history to third-parties, how is it doing so: in sharp detail revealing everything on a store receipt (e.g., purchased red cotton sweater, size large, on 12/20/95, for $49.95, with Visa), or in greater generalities (e.g., purchased women's apparel). Is the company disclosing the information only to corporate affiliates or to third-parties? Are these third-parties in a similar line of

business? Is the company using the information in unexpected ways inconsistent with how an average consumer might expect the information to be used?

Step # 4: Understand the contractual approach.

{16}As I had alluded earlier, the IITF promulgated a set of privacy principles, which are to be a model code for all participants, both public and private, on the NII. The principles and commentary, well worth reading in their entirety, have at their core the Notice and Fairness Principles.

{17}The Notice Principle (II.B) says exactly what you think it might say. It states:

{18}Information users who collect personal information directly from the individual should provide adequate, relevant information about:

- Why they are collecting the information;
- What the information is expected to be used for;
- What steps will be taken to protect its confidentiality, integrity, and quality;
- The consequences of providing or withholding information; and
- Any rights of redress.

{19}The related commentary adds that the type of notice must be sensitive to context. At times, "the ordinary and acknowledged use of personal information is so

clearly contemplated by the individual that providing formal notice is not necessary." For example, if a pizza parlor collects name and address over the telephone solely to deliver the right pizza to the right person, it will only irritate the hungry customer to hear an elaborate, explicit notice about information privacy. On the other hand, if the pizza parlor discloses the names of people who eat too much pizza to insurance companies trying to avoid health risks, then explicit notice would be necessary.

{20}The second core principle is the Fairness Principle (II.D). That principle states:

{21}Information users should not use personal information in ways that are incompatible with the individual's understanding of how it will be used, unless there is a compelling public interest for such use.

{22}The commentary defines the "individual's understanding" as encompassing "the individual's objectively reasonable contemplation and scope of consent when the information was collected." This, in turn, is determined largely by the information disclosed pursuant to the Notice Principle, discussed above.

{23}When joined, these two principles form what may be called a contractual approach to solving privacy problems. To use the lingo of contract law, the Notice Principle makes sure that there is a clear implicit or explicit "offer" by the information collector regarding the subsequent collection and use of the individual's personal

information. The individual's decision to go through with the transaction, for instance purchasing the widget, acts as an "acceptance." Offer, acceptance, and the exchange of consideration create a sort of privacy contract ("the individual's understanding") that governs how personal information may be used. Finally, the Fairness Principle, requires information users to obey that contract, not to use information in ways incompatible with the individual's understanding. Before information may be used in ways incompatible with this privacy contract, subsequent consent, at times implicit, at times explicit--must be garnered from the individual.

{24} There are venerable strengths to this market-based contractual approach. For instance, markets generally reach efficient results with minimal governmental interference. Markets generally give people what they want. Those who treasure their information privacy will get it. Those who care less, won't. But contractual approaches suffer from equally venerable weaknesses. Markets do not always work. In economics jargon, information asymmetry, high transaction costs, and monopoly power may prevent efficient results. Furthermore, even when the market reaches efficient results, it may fail to promote adequately other values such as fairness and distributive justice. In other words, privacy might be available in the market, but you might have to pay a lot for it. And the poor--assuming that they can patch into the NII in the first place--may be unable to afford even basic privacy protections that we as a society want all to share, regardless of wealth.

Step # 5: Check whether the contractual approach is working.

{25}The contractual approach may not be working in the status quo for two reasons. First, it might not even be in place. For example, information collectors might be collecting personal information from individuals without satisfying the Notice Principle. Or, they might be disclosing and using the information in ways inconsistent with the individual's understanding, in contravention to the Fairness Principle. My impression is that this accurately describes how a substantial portion of personal information currently flows on the NII. The contractual approach simply cannot ensure the appropriate amount of privacy if the individual is never even given an "offer," or if the privacy contract is honored only in its breach.

{26}Even if the contractual approach is in place, the market structure might be such that the contractual approach does not provide adequate protections. Take severe imbalances in bargaining power as an example. If you are the only telephone network or interactive television operator or widget manufacturer in town, then an individual customer will have little choice but to accept whatever privacy terms are dictated. The customer cannot simply walk away because there is no one else to walk to. This is one case in which the FTC's expertise in competition and consumer protection can come to bear together.

Step # 6: Implement a solution strategy.

{27}Three basic options exist here. I list them in order of increasing intervention in the marketplace.

{28}**Option #1:** if the contractual approach is in place and working fine (determined in Step #5), then do nothing. This is a policy maker's best case scenario. Individuals are being informed pursuant to the Notice Principle. On the basis of such notice, they are making intelligent decisions on whether or not to enter into various transaction, and information users are respecting the privacy contract in accordance with the Fairness Principle. In this environment, an individual's claim to control the terms under which personal information flows on the NII is being adequately respected.

{29}**Option #2:** if the contractual approach is not in place but would work fine, then mandate the contractual approach by instituting the Notice and Fairness Principles. In other words, simply mandate what the IITF Principles already recommend. No greater interference in the marketplace is necessary.

{30}**Option # 3:** if the contractual approach does not or would not work, then mandate minimum substantive privacy protections. As suggested above, the contractual approach may produce unsatisfactory results, in terms of efficiency and equity. In such cases, policy makers should enter the marketplace and shore up a floor

of privacy protections. One obvious place to start is to balance any inequality of bargaining power between information collector and individual. This may be achieved by requiring information collectors to acquire consent from the individual before personal information is collected, disclosed, or used in any manner not reasonably necessary to the successful execution of the transaction. This would guarantee that the individual is never forced to walk away from a transaction or service because of unattractive privacy terms.

Conclusion

{31}In closing, I want to highlight that this six-step process is far from a perfect algorithm for thinking about privacy. In this brief space, I have not provided nearly enough detail in which the devils of policy work their mischief. Nevertheless, this primer helps to create an analytical framework to help shape privacy initiatives. Importantly, this is a framework that draws from the most recent Executive Branch thinking on the matter.

{32}As the NII and the Global Information Infrastructure become daily more a reality, increasing interactivity and decreasing information processing costs will ensure that more and more personal information will be collected and used. Information privacy, aptly characterized as a consumer protection issue, will be at ever greater risk. The Federal Trade Commission should be applauded for its leadership in taking a hard look at these difficult issues now.

Date of BLT Publication: January 23, 1996