PRIVACY NOTES VI

Privacy is a topic of many facets. Its concerns are coming to illuminate more and more of the activities and transactions of our day to day doings. Two of these much in the news, are the subject of the present notes: it is hoped that our commentary will contribute something new to your information and your thought.

First is the perennial swarm of doubts and plaints surrounding medical records and their hoped for inviolacy. The annual conference on health care privacy organized by Deborah C. Peel's (Note: Dr. Peel also appeared as a medical privacy speaker at Dialogue on Diversity's recent Health Care Symposium, May 15) Patient Privacy Rights organization, was held June 5th and 6th. One of the sessions, perhaps the most technical and at once fascinating, dealt with the device coming to be known as "segmented" data with respect to patients EHR (electronic health records). The panel was moderated by Scott Weinstein (who had presented an exposition on this topic at Dialogue on Diversity's 2012 HC Symposium). The problem is that medical operatives, whose number, identity, and detailed future information requirements are not known in advance. At the same time each patient, with respect to the voluminous and widely varied information in health records, may wish not to make certain parts of that information (conceivably, in an extreme case, almost all of it) available to some medical operatives in a broad range of circumstances. The ban, thus put, is not absolute or invariant across classes of providers and types of medical circumstances, and specifically the gravity and emergency character of the circumstances. IT experts have begun to pick apart this tangle of contingencies and to design rules contained in the EHR software itself for disclosing certain pieces of a medical records to certain providers under certain circumstances. For example, if the patient is brought on to the hospital emergency crew in one piece but in a severely damaged condition, and had previously ordered secreted as objects for disclosure, say, a previous surgical procedure, certain previously used medications, and a previous substance addiction, and suppose then that the emergency procedures can be efficiently and safely performed only if the medical personnel have at hand exactly that embargoed information. At peril of the patient's being gravely disabled or dying should the bans not give way for the emergency physician, and at that only for the time of the treatment? At this point a further factor may be mentioned: should only the physician know or should assistants or, say, hospital record keepers know? The panelists presented in turn three systems now being tested, for accomplishing this complex sorting and gaming program. The system probably cannot operate successfully, however, without a certain kind of nuanced judgment of an intervening human participant. An example given by the panelists might be a prohibition of reference to a substance addiction; in compliance with this prescription substantial material relating to the addition is blocked, while at some point in the records mention, say, is made of a medical institution known to be specialized to addiction treatment. This too, while not referring expressly to "addiction" would be marked for elision. The instructions built into the system for spotting materials on the blockage list would be intricately fashioned and would be designed to cast a wide, but accurately delineated net, while the human review of the records would not be out of place, as noted. Part of the "emergency" character of certain circumstances would be the omitting, for the sake of speed, of this stratum of review.

This research is being conducted by, and under contract with, the Office of the National Coordinator for Health IT in the Department of Health and Human Services. It is a significant part of the larger project, taken in hand principally by HHS, for effecting the general, country-wide adoption throughout the health care industries of information technology instrumentalities. It is almost surely part of the coming IT configuration in the health care field. What is – if one steps back to view this project in a broader context – a gripping feature of the project is that it does not stop with the choice, on a balancing test, between privacy and efficiency, but through technological innovation a much greater quantity of privacy protection is achieved along with enhancements of efficiency.

A second privacy quarrel, always present but subject to sudden flareups, like that of the last two weeks, brings once again into special focus the proposed "trade-off" between safety – from potentially dangerous non-domestic persons or organizations – and the privacy interests of individuals. This has as its subject the recent disclosures of the dimensions of government data collection, which appear to be broader than had been commonly thought. We are not concerned here with the motives or character of the agent believed to have brought the latest intelligence to light, but with the impacts on privacy from the sort of systematic government data collection that is probably in train. Data mining, the indiscriminate netting of the vast volume of communications information, the date, destination, length, frequency of classes of communications, or indeed the content of communications – the accessibility to governments of all these, have been in the public consciousness for some time. It is scarcely a surprise at this juncture that such gathering is in fact going on in certain swaths of the communications universe [say, communications with one end outside the U.S.], and that the technical capabilities for collecting in other parts of that universe [say, conversations with both ends in the U.S.] presumably can been readily brought into play. One is still mostly in the dark as to the reach of the actual data collections, past and present – while speculating about the somewhat ominous prospect for the future. What is a bit more certain, however, and not quite so heavily shrouded in secrecy, is the existence of massive data collection by large commercial entities, first the carriers and firms in the internet service industries, and then retail and other firms dealing over the internet with broad portions of the national population. These non-governmental entities daily amass huge arrays of facts about subjects numbered in the millions. This mass of data now gets put to use for activities profitable for its possessors (and arguably useful to the subject customers and others), but might, again, be turned to uses detrimental to these subjects. Portions of this data trove could conceivably be obtained, moreover, by public authorities through subpoenas, court orders, or indeed extralegal means if a future government determined that a worthy project would be usefully advanced by commandeering the information – which would permit the succeeding holder, by hypothesis an intrusive governmental actor, to delineate the movements, proclivities, and the history, ornamented with its many achievements and peccadillos, of the social atoms that constitute the strength of the country. The very existence, in any present state and in the custody of any present possessors, of any portion of this corpus of data raises some further preliminary questions: how much data is held? and how long is the corpus maintained – with an expiry, or erasure date in six months, or a year, or will it remain as a perpetual trove? The longer it is kept, the greater the likelihood that sensitive personal materials could be made accessible to public authorities (for example, the formation of personal histories over some span of time). This may be profoundly worrisome since the public authority differs from any private sector entity in that, in the structure of society, it is the former that holds a "monopoly of coercion".

The crux of the danger lies in the very fact that the trove of data exists, whether initially in the hands of a governmental agency, a commercial enterprise, or an information technology service company. Data tends to be fairly fluid – large quantities can be shunted about quite speedily. And, as noted, its location is determined by governmental commands, informal transfer agreements, or through employment of surreptitious means. Again, means exist for preserving data, short term or indefinitely, and preservation could be inhibited, but ultimately not prevented by governmental prohibitions, commercial agreements, etc. In a historical perspective, dangerous hardware and processes exist in many realms, and have for long – guns, poisons, and other highly destructive instruments. Social pressures, legal sanctions, interdiction of supplies, inspections, etc., in an elaborate and slowly accreting patchwork, have been put in place and a rigid social ethos has formed inhibiting use of the dang erous gadgetry. Could something of these ethical mechanisms effectively enforce a protocol of proscriptions barring various privacy-abusing practices in the use of information technology? All this would help, but one must nevertheless seek to rely in great part on technological devices to stop these. One will be pressed willy nilly into the age-old rhythm attending the advent of dangerous instrumentalities: the initial, potentially harmful

technological advance, a growing abuse of the innovation, and a technologically contrived remedy fashioned in response, only to be succeeded by refinement of the original nefarious technique to circumvent the remedy – the battle is never won, but the evil, with a bit of luck, is kept at bay.

The papers have been filled with articles on a cluster of topics surrounding this larger question of privacy in the face of an insidiously penetrant information-gathering technology. Some have explored the availability of devices and techniques for circumventing the prehensile programs for cadging the clues to your personality and doings. These have an appeal for the persons who ruefully reflect that the commercial entities that have assiduously picked out the fragments of data and painted the portrait of one's life, tastes, and times, and have so wielded the story that they now – it is scarcely an exaggeration – know more about me than I myself. This is eerily reminiscent of St. Augustine's wonder as he realized that God is closer to him than he himself [Conf. III.6.11, "tu autem eras interior intimo meo" – lit. "you were more deeply within me than my own inmost . . ."] Is it an offense, without need to say more, that Google and, worse, the government are trenching on the divine prerogative?

The sheltering techniques are for the most part some form of encryption, but, it is noted, the strong forms of encryption that would be effective are costly and difficult to manage, would require that one's interlocutor be outfitted with the corresponding encryption system in order to "read" your transmissions, and that there be no point in the transmission chain at which a portion of the message is accessible in a non-encrypted form. Still another strategy for foiling the government's project of assembling a full and rounded portrait of the subject is the use of several e-mail systems, with distinct user profiles, and no mixing of cross references. Some division of subject matters is part of the trick – one system for business, one for hobby, one for family, etc. – the best the snooping entity could do is to assemble a set of fragmented snapshots, which could not evidently be matched with the others pictures of the set.

Another line of discussion takes up the underlying question, whether the privacy that is liable to be abridged, is a value that is itself intrinsically desirable or whether its concerns are activated only when a tangible loss arises or other specific harm becomes evident. Gideon Rachman, for example, recently suggested, writing in the Financial Tines, that the notion that others are privy to one's information, so long as they are remote and invisible, is not so disquieting, but that if a breach of medical record security gets one ejected from a job opportunity or the like, the want of privacy protection, only then, will begin to bite. Charles Lane writing in the Washington Post, questions whether privacy is any sort of "core value", or, again, whether it is a probabilistic shield against any of a variety of actual harms that may, now and again, in greater or lesser acuteness, come one's way. Thus the relative lack of widespread outcry over the realization that companies and governments are well advanced in compiling dossiers on us their customers and subjects. The nexus between the shield and the evil that it stands to avert is not sharply etched in the mind with the larger number of our compatriots.

And the further considerations re privacy are that a course of commercial data collection and analysis may channel to the subject buying or other desirable opportunities (and at once displace alternative advertising that would be of no interest to the subject), and that in the case of governmental collection, some sense, however diffuse, of enhanced "security" may be a positive benefit, to be weighed against the detrimental sides of the practice. The former, private-sector data collection is openly carried on for profit making motives by the internet advertiser, and the subject's holding still for the development by the advertiser of analytic conclusions may be viewed, with some plausibility, as the price consensually paid for the benefits. Against this last, however, is, again, the possibility that the existence of the stores of raw data could, if preserved, prove to be the instrument, in the hands of a future, less well-intentioned possessor, an instrument of oppression.