Privacy Notes II

The abbreviated comments below, signaling Dialogue on Diversity's continuing concerns with the proliferation of privacy puzzles, form the second issue of Privacy Notes, the string of mini-reports and analyses, however fragmentary, which, with luck, may formulate queries that the wits of readers will essay to answer, but may at the least pique the attention of a readership perhaps not always as sensitized to the cluster of privacy issues as a due prudence in our fragile age might commend. News this week: first an article in a recent (3.13.12) Politico – attention is drawn to the brewing disputations on the anatomy of "tracking" and the contentions of the parties in interest over the proper rule for its forms, frequency, and uses. Next is a conference just held in Washington, Monday, March 19, airing the content of a draft proposal designed by the competent authorities of the European Union to establish the architecture of privacy for communications within the EU and between the confederation and the outside cosmos. Attention then turns to a more specific discussion of certain elements of the recent White House White Paper on Privacy (mentioned in the earlier Privacy Notes). Finally: the alarming tidings that job applicants are being invited to turn over to HR their social network password[s].

I. How Close on Your Trail May the Trackers Tread?

The FTC waits watchfully as several leagues and associations of players in the "tracking" industries – the internet carrier/content-originating/data-analyzing industries – mull over the questions of information collection practices – whether they ought to track at all, whether if only with the opting in or opting out of subject users, with efforts undertaken to anonymize the data as to users' identities, and whether such data as does get collected may be used to target marketing ploys to particular users, once they have been sufficiently psychologized. And if it be agreed that collection is licit if not used in targeting commercial appeals, then what is the collection for at all? Well, for one thing, to spot fraudulent use of credit cards (the instant purchase, a computer in its wisdom might conclude, is so unlike this particular user). The rules specifying the bounds to permissible collection (kind of users, kind of data, degree of identification of users, permissible collation and analysis of the information, the acceptable uses of data, etc.) – these are being refined by discussion, indeed negotiation, among the firms collecting or trafficking in personal data on internet users. With the FTC waiting to contemplate the result and determine whether the system so evolved can be gauged consonant with governing statutes, and with the nicely articulated sense of justice in the agency. Cf. provisions of WH Privacy White Paper, below, III.

II. The Call for a Comprehensive Policy: the Nations Ascend the Bandwagon

The White House privacy statement, discussed below, is roughly contemporaneous with the European Data Protection Regulation, a measure proposed for the EU in the nature of reform to existing rules and practice. The proposal confronts a state of affairs on the continent not unlike the present state of privacy protection in the U.S, where existing regulation forms a tolerably satisfactory texture of privacy protection in certain dedicated fields, but leaves interstices where regulation of any comparable specificity is wanting, while at once allowing disparate standards of privacy to operate in many similar classes of transactions. The new standards put forward for consideration within the EU direct the most urgent attention to those pools of less well covered transactions, intending to shore up the barriers against intrusions on the privacy space of affected individuals. The proposed comprehensive, logically even-handed rule would provide, among other things, a right to opt out of tracking or other collection practices, a right to require excision by internet providers or carriers of certain data touching one's affairs (the right to "forgetfulness"). This array of rules, while each seems to achieve a cognizable value, are subject, clearly enough, to objection, which in fact is coming at high volume from the side of the content originators/data collectors, whose economic viability depends largely (under existing business models, at any rate) on the collection and exploitation of just this user data. The industry affected has made known its reservations respecting the novel rule. Doubtless an all-embracing rule will, in the event, be placed in force throughout the Union, but the precise shape and the rigidity of its provisions will be majorly massaged in the season of debates lying just ahead in Europe – and in the U.S. as chief correspondent.

III. The White Paper on Privacy

The widely publicized white paper on privacy policy, issued very recently by the White House, and indeed over the signature of the country's chief executive, immediately confronts the reader with the difficulty of dual goals in a purportedly coherent policy directive. Query: whether this high sounding proposal is in effect the recipe for a zero sum game – with a substantial enhancement of privacy coming only at a loss of comparable value, somehow measured, in the innovative goads that propel American engineers onward and upward in the IT enterprise – or whether some exertion of technological ingenuity may manage to achieve a suitably high level of privacy enjoyment alongside a respectably brisk innovative impulse. A proponent of any such policy formula must seriously deal with this question. The analogous

quandary, it will be noted, continues to generate heated disputes over the dual mandate of the Federal Reserve System (how to mix the initiatives designed for price stability with any initiatives calculated to maintain full employment). A serious statement of what purports to be a coherent policy would at least outline a plausible formula for harnessing these two goals, or sets of initiatives, to a single cart amenable to the management of a single teamster. The White Paper, over a hundred pages in length, can be brought up swiftly by several judicious clicks with Google.

Another remarkable feature of the White Paper is its proposal that firms in the telecommunications/IT industry should work out their own agreement on prescriptions for the privacy problem, the agreement to be enforced, once it is concluded, by the FTC. This prospect brings an eerie echo of the Industrial Codes of the 1930s, in which a variety of industries were virtually cartelized with rigid performance dictates, formulated by each of the industries themselves, often designed to impose higher prices on the body economic. The danger in the present case, that of the IT industries, of setting up a cushy arrangement for existing firms is compounded by the fact that, contrary to the state of affairs in 1930-vintage American manufacturing, the present IT industries are remarkably fluid in technologies and business models, and, therefore, in players. Any rules should thus take account of this "moving target" element as regulatory initiatives are designed.

IV International Summit II on Health Privacy Policy

June, 2012 , will mark the first anniversary of the original International Summit on Health Privacy Policy, this 2012 edition to be held again in Washington at the Georgetown Law Center on New Jersey Avenue. The title: *Is there an American Health Privacy Crisis?* Among topics to be dealt with by the first class experts on the agenda: health/medical data by way of "cloud" technologies; the effects of the U.S. and E.U. policy projects mentioned above in these Privacy Notes; data exchange and secondary use of health data; and more. Dialogue on Diversity is happy to partner with the organizers of this forum on health data and the privacy conundrum. Readers are directed for detailed information on the occasion to www.healthprivacysummit.org

V "Apps", the Mole in the Hand-Held

Regulatory and legislative authorities, from California cities to the Congress in Washington, are sensing the incipient alarms over newly revealed privacy perils in the technology of contemporary smart phones as they bear the assault of the ubiquitous "apps" that are marketed on every hand for installation on iPads, mobile devices, and, most notably, the proliferating population of "Smart Phones". The devices – the "apps" – in question are the specialized software packages that perform a narrowly demarcated function or service – games, tools, social network entree, etc. – to be evoked by a flick of the mobile device user's finger. Newspaper research articles have recently publicized the gaps in the operating systems of some of the most widely used gadgetry. Reports are cropping up of penetration obtained by ingenious hackers to users' address files, photo files, and other materials accessible from or through the phone. This vulnerability is especially worrying (Sen. Schumer confesses that the thought of it sends shivers along his spine) since increasingly it is smart phones that are the repository of massive quantities of the user's information, and of all the identifying data. Some suggestions for regulation would impose privacy standards on the developers of the apps, while under another view, the retail stores that purvey these would be targeted as the chiefly responsible entities – the entities standing at the point in the chain most readily situated to police the ingenuities of the developers. The show goes on, and promises to grow ever more interesting as time goes by.

VI Encroachments: Privacy is Disclosure – When, Where , and To Whom?

A flurry of disgruntlement with the quirky paths of a free economic system has followed news that some employers, public-and private-sector both, have commenced to solicit job applicants for one's social media access keys, user name and password. How badly do you need the job? With a shrug of the shoulders fork over the secret number? Or should the new national anthem be the tartly phrased lyrics from the venerable American Songbook: You Can Take this Job and Shove It. There are always, to be sure, many sides to any controversy. Several questions: how many cases exist of such intrusive requests? Is it a growing trend or a very few isolated aberrations? (Is it different in kind from the long-standing practice of a good many domestic relations lawyers of seeking to discover all, not some, of the opposing party's diaries – one of the incidents of legal practice that, among many others, have brought the law into disrepute?) And indeed is it a reminder of the wisdom that guided us before the social networking sites took over American culture? that there is much to our histories and inner souls that are the *tacenda,* the things that are not spoken if not safely within the circle of the closest and most trusted persons (not more than three or four at the outside) – and after a check that none of them at that are bearing tape recorders. Privacy, after all, is not absolute non-disclosure, but the power to control *when, where,* and *to whom* this or that particular may be displayed and spoken of.

1629 K Street, N.W., Suite 300, Washington, D.C.
Tel: 703-631-0650 Fax: 703-631-0617
dialog.div@prodigy.net www.dialogueondiversity.org