www.jusletter-it.eu

Orlan Lee / James She

«It Could Never Happen Here!»

Changing Circumstances Affect U.S. Personal Data and Privacy Law; New Forces Preserve What Suits Them for Themselves

We have realized for many years that, with advances in technology, we were subject to surveillance of unknown kinds from unknown sources. Nevertheless, revelation of the extent of surveillance by our own government comes as a shock. Layman's indifference to technology has also allowed a private sector culture of profiting from exploitation of access to private personal data to emerge. To callous personal data specialists, special interest law «liberates employers from following the [law's] exacting consent and disclosure requirements» when investigating supposed «employee misconduct». Not even the police have powers like that in the United States.

Category: Articles
Field of law: Data Protection; Data Security
Region: United Kingdom; China

Citation: Orlan Lee / James She, «It Could Never Happen Here!», in: Jusletter IT 15 May 2014

ISSN 1664-848X, http://jusletter-it.weblaw.ch, Weblaw AG, info@weblaw.ch, T +41 31 380 57 77

Inhaltsübersicht

1 Introduction

[Rz 1] Disclosure of the surveillance tactics of the National Security Agency reveals – as was perhaps long suspected – that the U.S. Government has been engaged in practices, to all appearances, at odds with the concepts of civil liberties Americans grow up with. To activists of civil liberties, and to defenders of strong action against potential terrorists or subversives as well, this revelation has ruffled our convictions that it could never happen in America.

[Rz 2] There was a time after the Second World War in which both liberals and conservatives shared the concern that we should never again allow government to seize the dictatorial powers over the individual that we had witnessed in Nazi Germany and the Soviet Union. In the 1960s and 70s there was, therefore, a drive for protective legislation to secure this goal – to promote open government, to protect privacy and civil liberties, and to prevent invidious discrimination. These laws became models for similar legislation in all the liberal democracies.

[Rz 3] A division soon arose, however, between strict libertarians and those anxious about loss of what they considered essential state powers. The division became greater, when it came to possible limitation of the powers of private sector entities to take up the promise of efficiency offered by the emerging new information technology – even where technology became highly intrusive into the private sphere. If consolidating personal data promoted greater efficiency in government and business, and offered new benefits in the financial and other commercial sectors it must be legitimate to make use of such advantages – or so it seemed to those who looked only to profitable means of implementing the emerging information technology and access to consolidation of personal data.

[Rz 4] It was easily overlooked that consolidation of vast amounts of personal data, whether in government, or in private corporate hands, has actually led to return to agency secrecy, loss of freedom of access, and the potential for hidden discrimination and invidious forms of stereotyping. Control over vast amounts of personal data, whether in government or private corporate hands, has meant the opening for potential abuse and loss of individual freedom.

[Rz 5] Unfortunately, there was to be no comprehensive law of Privacy or of Ownership of Personal Data in the United States – such as are now appearing in the EU and Commonwealth countries. Memory of the secret police states of the war years gradually faded and the fear of personal surveillance was never known by the generations of Americans that followed.

[Rz 6] Development of the new Social Media has also led to what the law calls «changed circumstances». It is not so much that the law has changed, as that it must now account for a new reality. The ability of technology to handle «Big Data» has created a new environment. We have not lost our traditional concerns about what we consider Private and our Personal Data. But, special interest legislation promoting «interactivity» on the internet, and «interoperability» of new technology, obliges us to speak in a new language. Yet, unless new legislation repeals, amends, or modifies the existing law, our traditional common law protections remain as they were – as long as we defend them. The extent to which the new legislation, or the existing law, applies must then be determined by the courts.

[Rz 7] Creative Business Communication has, meanwhile, led to innovative ways around the law... extracting «Waivers» of Basic Rights from consumers in take-it-or-leave-it contracts for rental accommodation, public utilities, financial services, employment, and computer software... leading also to commercial surveillance files, often based on mere gossip and hearsay, on every man, woman, and teenager in the United States. And, these files exceed the volume of the secret police files of the dictatorships of the 20th century. Whether Law or Business wins in the end will be the lesson we learn from dealing with the more deceptive Business English promoting only the exploitative aspects of the innovations in Social Media of the last half-century.

2 «Interactivity» as Goal of the New Media

[Rz 8] *The Telephone and the Loud Speaker:* A talk show media pundit recently attributed the growth in social «interactivity» in the early 20th century to the first IT revolution, the invention of the telephone. «By contrast», he joked, «after the Russian revolution the Soviet state relied on the loud speaker». The point was that the Western «democratic» ideal is one where we put great store in developing as individuals, pursuing our separate ways and business. Our streets and cars and classrooms are full of individuals telephoning each other. Opposing ideologies that consider themselves «social-minded» tend to be more grateful for means to call out mass demonstrations. Practically speaking, however, it is not the IT that adapts itself to human ideologies. We adopt the IT suited to the communication needs we are pursuing at the time to suit our own purposes.

[Rz 9] «*Internet Freedom*» *and* «*Censorship*»: Users of «social media», or new means of internet communication, today, often seek access to exchange of ideas, words, and music, across a wide range of friends and contacts. The new medium of exchange encourages, or is promoted by, the concept of «*internet freedom*», the notion that the internet was «born free» protected from the society around it. Enthusiasm for the new medium can lead us to ignore traditional legal standards of *copyright*, *defamation*, *suppression of pornography*, etc. Sudden re-appearance of authorities seeking to control access to materials, more tightly controlled in print media, sometimes leads those affected by social controls from the past to regard this as «*censorship*».

[Rz 10] Lawrence Lessig, a radical activist law professor, is famous enough that as «netizen» he can speak of a need for a «free culture», «free software», and a «free internet». It would certainly promote greater internet democracy to have the wider access to «open source» material and new means of «spectrum allocation» he advocates. He is in favor of innovation. But he does not believe in extended periods of ownership of patent and copyright, which he believes hinder the ability of other gifted persons from developing further the achievements of the first generation of innovators.

[Rz 11] In the rhetoric of the digital age «internet freedom» sounds as if it were not subject to the same laws as other media. But, that is exactly what «freedom of expression» means (as Professor Lessig is well-aware, when he wears his hat as law professor) – that is, that «freedom of expression» is *not* «a state of no-law», but a condition where law protects *intellectual property* (e.g., by *patent* and *copyright*), and also where the laws protect *personality* (i.e., by law of *defamation* and law of *exploitation of name and image*).

[Rz 12] Lessig as «non-netizen» also admits, that if present constraints on «internet freedom» and communications technology were gone, «*other interests [would] take their place*». Unspoken here, is that the internet and the realm of information technology conceal within themselves countervailing internet-internal controls by operators of the medium itself – *favoritism in search selection*, *tracking of web-surfing*, *scanning of e-mail*, and the *planting of adware and malware*. These practices shape the results we achieve in use of the new medium far more than protection of intellectual property and prevention of defamation.

[Rz 13] In other words, we are talking about how the ordinary common law applies on the internet. There are negative forces at large as well. But if «freedom of expression» (guarantied by the First Amendment to the Constitution in the United States) is what we are after, we deceive ourselves if we attempt to drive out the limits of that law that prevent us from defaming one another. These limits include both protection of certain intellectual property, and prevention of certain attacks on personality. It is an ancient proposition of lawyers that we look for protection of «*liberty under law*». We are «*born free*» only in the jungle.

[Rz 14] *Who Owns the Internet?* In addition, if we neglect the vital question of «*who owns the internet?*» we omit entirely consideration of the fact that, outside internet cafes, universities, and public libraries, where we are permitted relative free access, *some of us may not be able to afford an internet connection at all*, or may be forced to subscribe to a «bundle of services» we are not interested in from monopoly «providers» (ISPs), in order to have access to the airwaves we believe we have a right to. **In other words, whether new innovations are adopted or not is a matter of the purpose they serve. In the end, «social media» and the internet, like the telephone and the loudspeaker serve their users» purposes.**

3 Privacy, Personal Data, and Freedom of Speech

[Rz 15] *Concepts of «privacy», «personal data», and «freedom of speech»* are, like the concept of «*internet freedom*» not «born free» of the society of law around them. All of them exist, to the extent they do exist, because of special protections evolved over time. What other country has ever taken as the opening words of its Constitution: «Human dignity is inviolable»[1]? But, the Germans did this only as the authors of their Basic Law recognized that the German state had only just emerged from the most violent abuses of human dignity in the history of civilization.

[Rz 16] There is no definition of «human dignity» in the Constitution of the United States. There is no definition of «privacy» or of «personal data», either. These are all concepts that emerged later in our history than the Constitution of 1789. But we can claim at least that all were implied, and that «freedom of speech» was expressly protected (though undefined) in the Bill of Rights,

[1] Art. 1.1 of the Basic Law of the German Federal Republic of 1949.

the first 10 Amendments. What these Amendments did was protect against the abuses already experienced: *search and seizure without warrant* (Fourth Amendment); *being forced to testify against oneself* (Fifth Amendment); *right to confront witnesses* (Sixth Amendment). All of these defined the nature of «*due process of law*» that ultimately led to the implied right to protection of «*privacy*».

[Rz 17] «*Freedom of speech*» *or* «*of expression*» is an esteemed right with ancient beginnings in the common law world that we consider essential to our modern way of life and the law. It is also at the heart of the development of «Social Media». But the principle of «freedom of speech» also exists within ancient and trusted bounds.

[Rz 18] In other words, «freedom of speech» is a principle of organized society, which also sets limits on it. There is no «freedom of speech» in the jungle – because there cannot be «freedom of speech» for one party. **There is no «freedom of speech» to destroy an adversary who cannot respond – to protect the «freedom of speech» of the opposing party, we have to limit the «freedom» of the adversary. And, there cannot be «freedom of speech» with total anonymity and immunity from liability.** Americans learned long ago of the need for restraint against «*falsely shouting fire in a crowded theater*». There are also vital restraints against *breach of confidentiality*, against *violation of fiduciary duty*, etc.

[Rz 19] *Special Interest Legislation:* Then is the expectation that the internet service provider must exercise *reasonable care upon notice* that it is distributing defamatory, indecent, or socially inflammatory material, so onerous to an ISP that it will not take these down? It sounds magnanimous at first to hear that Congress has extended «total» «freedom of expression» to what is said on an «interactive computer service» on the internet. The flaw in that logic is that that «freedom» is one-sided. Its supporters require that it be both anonymous and immune from all liability.

[Rz 20] If in enthusiasm for new media we cast off whole sections of the common law that time, logic, and the public have designed and legislated for our protection, have we considered what we are putting in their place? Lobbyists for special interests have succeeded in, for example, making a cultural idol of the supposedly unique interactive qualities available on the internet. Ironically, we read in a special interest sponsored law, with the misnomer «The Communications Decency Act»[2], that the normal limitations of good taste can be set aside for the sake of «interactive» communication on the internet:

> It is the policy of the United States – (1) to promote the continued development of the Internet and other interactive computer services and other interactive media; (2) to preserve the vibrant and competitive free market that presently exists for the Internet and other interactive computer services, *unfettered by Federal or State regulation*[3] (italics added).

[Rz 21] «*Unfettered by Federal or State regulation*» was clearly not meant to require abandoning all restraint. Further on in the same section we read that a person who does act to protect the public interest «voluntarily», not with the force of law, is relieved of liability under this very law that removes federal and state regulation:

> No provider or user of an interactive computer service shall be held liable on account of – (A) any action voluntarily taken in good faith to restrict access to or availability of material that the provider or user considers to be obscene, lewd, lascivious, filthy, excessively violent,

2 Sec. 230 of The Telecommunications Actof 1996.

3 47 United States Code [USC] §230.

> harassing, or otherwise objectionable, whether or not such material is constitutionally protected; or (B) any action taken to enable or make available to information content providers or others the technical means to restrict access to material described in paragraph (1).

[Rz 22] In other words, if the operators of an ISP do entertain social moral reservations about some of the rubbish on the internet, they *would still be «unfettered by regulation»*, if, out of *their own scruples*, they took down offensive material, or if they informed concerned parents on how to block it. Yet, if the ISP has no such scruples, it has been held that they can calmly ignore how harmful any material is that others have put up.

[Rz 23] Accordingly, the ISP was relieved of liability under part (A) of section 230, in a case where both parties agreed that defamation and an attack on the reputation and livelihood of an apparently totally uninvolved third party had taken place, where a person was accused on the internet of deriding and profiting from the death and destruction that had occurred in the worst terrorist act to occur in the United States prior to September 11, 2001, the random bombing of the Federal Building in Oklahoma City in 1995. Yet, the ISP would have been equally free of liability under part (A) had they been moved by the scruples that the law would otherwise have demanded if the existing law had not been neutralized by section 230 (2).

[Rz 24] There was no apparent motive for the highly damaging personal attack on an unrelated third party. Yet, AOL, the internet service provider carrying these defamatory postings ignored many requests to remove them regardless of the severity of attacks on the victim and his livelihood – regardless of death threats arising from the postings and the need for police protection around his home[4].

[Rz 25] Special interest legislation had made the ISP immune from liability, probably we can say because the American public relies on its elected representatives in Congress to deal with such matters, and often is blindly unaware, or deliberately misled, regarding the possible impact of such departures from the common law. Costs for the victim, damage to his livelihood and reputation, and threats on his life notwithstanding, the Court itself cited counsel for AOL that the ISP would not be liable,

> ... even if AOL knew of the defamatory nature of the material and made a decision not to remove it from the network based on a malicious desire to cause harm to the party defamed[5].

[Rz 26] *Conflicts of Laws:* The Court's summary of the law in the case, as cited by Zeran, is obviously nonsense. The obligation to remove a defamatory publication upon notice is otherwise embodied in the law. And the malicious desire to cause harm clearly results in tort liability. If the Court finds an exception in this case, as it believes it must on the basis of section 230, it is nevertheless still obliged to define and justify it.

[Rz 27] **Unless a new statute repeals, amends, or qualifies an older statute or rule, then both remain in effect. Congress created an exception, but did not repeal or amend the laws of defamatory publication or of malicious tort liability. The extent to which all these conflicting laws apply at the same time, and under what conditions, is, therefore, left to the Court to define.** That principle was laid down in Marbury v. Madison (1803), the ancient case that defines the meaning of rule of law in America, and obliges the Courts to resolve differences in conflicts

4 See,Zeran v. America Online, 129 F.3d 327 [4th Cir. 1997].

5 Cited by Zeran in an address at the *15th Anniversary Conference of 47 Section 230 U.S.C.* held on March 4, 2011.

of laws. However, in this case, the U.S. Supreme Court also declined to resolve this dilemma[6].

[Rz 28] It is not just the legal absurdity of the final assertion by the Court of Appeals in this case that deserves our close attention. We should also be concerned that legislation drawn to serve special interests sometimes produces such arrogance – and, as apparently in the *Zeran* case, the Court just as arrogantly went along with it. [**The reader may think that the Court is justified in blindly following the logic of the Communications Decency Act. The authors reject the notion that special interests can simply carve out exceptions in the law to suit themselves. If Congress insists on taking the risk that one statute nullifies another – leaving us with clear and serious gaps in the law of tort and defamation – let them say so**.]

4 Why Should Social Media and E-Commerce Require «Waiver» of Personal Data Law to Thrive?

[Rz 29] *Take-it-or-Leave-it Contracts:* The *Zeran* case has gratefully been unique. Thus even despite its unjust outcome, it has not been widely followed. That has not been the case, however, with a long line of take-it-or-leave-it, or «clickwrap», contract cases. In these cases, it is not Congress or the state legislature that has taken away the rights of the individual (as in the ineptly named Communications Decency Act). Rather, in these cases, the individual is supposedly *obliged to* «*waive*» *his or her rights* by «clicking on» and purportedly accepting «Terms and Conditions» that the courts have not, on occasion, hesitated to call «unconscionable».

[Rz 30] The pitfalls of special interest e-commerce law are nowhere better illustrated than in the case Comb v. PayPal[7]. PayPal is an internet payments system that was created by a number of electronics geniuses, innovators, and entrepreneurs, that allows individuals to make payments through an electronic intermediary that draws payment from the bank accounts, and credit cards of its subscribers, or from separate cash accounts they open with PayPal. To outward appearances, PayPal is able to transfer funds securely without revealing those subscribers» bank account or credit card numbers (at least outside the trusted circle of the financial institutions). It is a popular and profitable system among financial institutions, each of which benefits from fees on transactions along the way. Yet, taking this case as an example, PayPal had neglected basic customer service. And the feudal legal relationships it imposes on its members through the 25 pages of its online «Terms and Conditions» take us back to the dark ages.

[Rz 31] *Definition of Contract*: By-and-large law of contract and law of tort (the body of law that assigns remedies and assesses damages in compensation for negligent or non criminal harm) have evolved in the Western democracies through the slow process of legal reasoning, not legislation. By judicial definition, *a «contract» is «something bargained for»*. It is voidable if it can be shown that despite appearances, there was *no «meeting of the minds»*. If there are special «Terms and Conditions», there must also be «*mutuality*» *in their application*. Of course we have become accustomed to solemnizing such agreements with a signed document. A handshake or another form of acceptance will also do – if the contract expresses the «meeting of the minds» where something of value has been «bargained for». Yet the typical internet «Terms and Conditions» agreement has very little of such much vaunted «*interactivity*». In that event, a court is justified in doing exactly

6 Zeran v. AOL, cert. denied, 524 U.S. 937 [1998].

7 218 F.Supp. 2d 1165 [2002], a class action.

what the court in this case did: hold the whole thing «*unconscionable*».

[Rz 32] *Compulsory Arbitration of Disputes:* Internet and financial services industry «contracts», today, typically require that all disputes be settled by arbitration. That is, the «Terms and Conditions» oblige the subscriber to forego the established institutions of law and the courts, and accept a law of contract expressed in the «Terms and Conditions» which only allows recourse to a commercial board of arbitration in the event a «dispute» arises.

[Rz 33] Doubtless, arbitration or mediation of disputes may have been preferable to litigation in the days of the traditional society, where restoration of good relationships, not victory over a point of law, was the primary concern. The same theory applies in disputes between nations or between large corporations. In those cases, where restoration of good working relationships is the primary objective, mediation or arbitration can produce satisfactory results at minimal cost. Where the «disputes», as in the *PayPal* case, are over alleged overcharges, withholding access to one's own funds held on account, payments to the wrong parties, etc., the subscriber is not looking for restoration of good relationships, but for proper remedies or compensation according to law. Furthermore, commercial arbitration (as opposed to, say, arbitration by tribal elders) is generally not a cheaper alternative to a lawsuit, as is often alleged. In fact, it can be prohibitively expensive.

[Rz 34] The U.S. Federal Arbitration Act (FAA), a piece of special interest legislation dating from 1925, makes it mandatory that once the parties have agreed to arbitrate their disputes (as the «Terms and Conditions» of essentially all financial institutions and online operators require today), they have waived their rights to go to court, unless the agreement itself can be set aside as defective. The FAA was supposedly promoted as a means of reducing the growing burden of litigation in the courts. In reality, it simply enables the financial services industry, particularly, to resolve disputes before arbitrators drawn from their own industry. Arbitrators, unlike judges and juries, are not bound to decide strictly on the basis of law. They do not have to write legal opinions. It is, therefore, understandable that internet and financial services companies prefer not to risk jury trials and state consumer protection laws, and put their faith in arbitration.

[Rz 35] *Unconscionability:* In the *PayPal* case, the Court found that the arbitration clause in the «Terms and Conditions» was both procedurally and substantively unconscionable. It was held procedurally unconscionable as a «contract of adhesion» (that is as a take-it-or-leave-it agreement for an essential service). And it was held substantively unconscionable by reason of other one-sided advantages for PayPal (for example, the right to withhold funds in clients» accounts during prolonged investigation of disputes; requiring that arbitration be held in Santa Clara County, California, regardless of where the customer was located; and prohibiting combination of claims in a class action). Plaintiffs also showed that arbitration was prohibitively expensive and resulted in most claims, each of which averaged circa $55, being abandoned. PayPal itself had reserved the right in their «Terms and Conditions» to go to court on its own claims, while subscribers were obliged to go to arbitration. Furthermore, PayPal was authorized to change the «Terms and Conditions» without notice, merely by posting such changes on the internet.

[Rz 36] Plaintiffs prevailed here. However, as is sadly frequently the case with prominent corporate adversaries, all the abuses complained of continue in PayPal «Terms and Conditions, to this day, and the «Terms and Conditions» of like organizations also continue just as before. Of course the *PayPal* case can be cited as precedent whenever similarly situated parties manage to avoid arbitration and are allowed to take their cases to court. Although the *San Francisco Chronicle* reported on this case, **the media generally do not report or follow up on such cases. The public, therefore, remains ignorant of the law, and there are, therefore, no changes in take-it-or-leave-**

it contracts and online applications and «Terms and Conditions».

[Rz 37] *Vagaries of the Electronic Funds Transfer Act (*EFT*):* Plaintiff number one in the *PayPal* case had not signed an agreement to become a PayPal customer. Yet, PayPal had deducted funds from his bank account without his knowledge (by virtue of still further special interest law, the EFT). PayPal acknowledged the error and eventually returned these sums. But PayPal refused to repay lost interest or bank fees for overdrawing Plaintiff number one's account. Plaintiff number two also had had funds withdrawn from her checking account without authorization and paid to four unknown individuals. When Plaintiff number two stopped payment to PayPal in another unrelated matter, PayPal informed her that they would draw funds from another of her bank accounts and from her credit card. A third Plaintiff also had his account with PayPal blocked as the result of errors in which PayPal had placed incoming payments in the wrong account.

[Rz 38] In all of these incidents, PayPal customer service was essentially unreachable, yet PayPal, itself, operating with cooperation of other financial institutions was unstoppable in the damage they could do to subscribers» accounts. **None of these EFT abuses should have occurred if financial institutions had exercised the same level of care in transactions initiated by other financial institutions as they do with transactions of ordinary customers.**

[Rz 39] *Binding Revisions of «Terms and Conditions»*: PayPal conceded that the agreement that Plaintiff number two had signed had no arbitration clause. However, there had been five different versions of the «Terms and Conditions» in the period Plaintiff number two had been a client. PayPal maintained that Plaintiff number two would, therefore, still be bound by the arbitration clause because she had accepted a provision that PayPal could vary the «Terms and Conditions» at will from time to time, and that customers had to keep track of these themselves on the internet as they appeared.

5 Decisions We Follow – Decisions We Ignore

[Rz 40] *What happened to the PayPal Decision*? No decision was made by the *PayPal* Court with respect to whether revisions of «Terms and Conditions» were still binding, having already found that the arbitration clause inserted in the «Terms and Conditions» of Plaintiff number two was unconscionable. The Court did say: «*PayPal's unilateral and apparently unfettered right to revise the User Agreement at will does bear on the question of whether the User Agreement is substantively unconscionable.*» This may be enough to lead the Court to conclude that such language would always be substantively unconscionable. The major issues had been decided. Yet, **there has been no equivalent change in the going «Terms and Conditions». And as long as the media and the business schools ignore these decisions, the financial institutions and all the companies with sharp business practices will force us to litigate the same issues over and over again.**

[Rz 41] *The «Miranda Warning» in Criminal Procedure Law*: The situation has been different in criminal procedure law. Government knows when it is compelled to follow the orders of the courts. Those of us who watch American TV have all learned that in the United States anyone who is arrested must be given a «*Miranda warning*» before being questioned by the police: «You have the right to remain silent, but, if you choose to say anything, it will be taken down and may be used against you.» (A similar rule exists in other English-speaking countries and in the EU.) Americans also have «*a right of access to a lawyer*». If you can not afford a lawyer, a lawyer can be appointed for you by the court. In the U.S. everyone has «*the right to due process of law*» *in criminal*

law matters. Of course, having a right to remain silent does not mean that it is the wisest choice to do so. *You may choose to waive that right for better treatment by interrogators*. «Plea bargaining» may not be the most uplifting characteristic of criminal procedure. But the individual is a lot better protected with the right to bargain than without it.

[Rz 42] «*Waiver*» *of Our Rights in Civil Law Areas*: But *there is no* «*Miranda warning*» when we «*waive*» *our rights* every day in civil law matters: in «*Terms and Conditions*» we never read – for renting an apartment, in opening a bank account, in subscribing to public utilities, in engaging in financial transactions, in downloading online apps, in subscribing to social media, and on and on. We do have rights in all these civil law areas as well as in criminal procedure matters. We may not be consciously aware of them. But *if someone is asking us to «waive» those rights in advance, there is obviously something to be gained by those who do not want us to know we have them.* We would all be better off, and there might be fewer monopolies, if we all knew that we could reject «Terms and Conditions» that force us to abandon our natural and legal rights.

[Rz 43] *The «Bill of Rights» Protects against Government*: In the United States, **there is constitutional protection against unwary disclosure of damaging personal data in criminal procedure matters:** we are *not obliged to testify against ourselves*, there is constitutional protection against «*search and seizure without a warrant,*» we have «*the right to know the nature of an anonymous accusation*», and we have «*the right to confront witnesses*» against us. The «*Miranda warning*» and the «*right to legal counsel*» in a criminal case protect us against the loss of the foregoing rights (in U.S. law these rights are protected by the Fourth, the Fifth, and the Sixth Amendments to the Constitution of the United States. There are similar rights in Commonwealth and EU countries.)

[Rz 44] «*Buyer Beware*» *in the Private Sector:* **The constitutional protections we enjoy in the criminal procedure areas apply against the police and government agencies. They do not ordinarily apply against private sector entities** – unless, as is bound to occur when we «waive» our rights in what appears to be an ordinary «investigative consumer report», in which it turns out we are accused of something they will not disclose to us, by anonymous persons we cannot confront. **[If Congress itself has no power to determine the «character» or «reputation» of every man, woman, and teenager in the United States – as U.S. «consumer reporting» law used in «credit reporting» and «recruitment screening» appears to allow, then Congress does not have the power to authorize any other entity to make a business out of it. Hopefully, one day this argument will be made before the U.S. Supreme Court.**[8]**]**

6 Who Does Our Personal Data Belong To?

[Rz 45] *No «Personal Data Law» in America*: Nowhere in American law is it laid down in so many words that a person has title to his or her own Personal Data. Instead, *for the most part we find that we are dealing with something the existence of which is only implied* by *the violation of various protected legal relationships*: that is Personal Data protection is implied by potential *violations of trust and confidentiality*, implied *in defamation* (that is, by an untruthful attack on someone's personality), and implied by *recognition of Invasion of Privacy.*

[Rz 46] *What You Can Not Say or Do*: On the other hand, Americans are used to the idea of the

8 See, O. Lee, .Lanham, MD: Lexington Books, 2012.

very broad concept of the First Amendment to the Constitution: «Congress shall make no law ... abridging the freedom of speech, or the press.» It is interpreted as the guaranty of «freedom of expression», though the Amendment does not use that term. (The Amendment does include «the right of the people peaceably to assemble, and to petition the Government for a redress of grievances», which is, of course, «expression».)

[Rz 47] The fact that Congress cannot make a law *abridging* «Freedom of speech» or «of expression» is sometimes, mistakenly, interpreted to mean that we can say anything we choose about whatever we choose. That is not true. As observed above, that ignores the specifically protected legal relationships of *trust and confidentiality*, *prohibition of defamation*, and *protection against invasion of Privacy*. Furthermore, as long ago as 1918, the U.S. Supreme Court held that «Freedom of Speech» would not permit «*creating a clear and present danger*»:

> The most stringent protection of free speech would not protect a man falsely shouting fire in a theater and causing a panic.[9]

[Rz 48] More recently, the Supreme Court appears to have lifted the level of presumed restriction from «*clear and present danger*» to «*inciting to imminent lawless action*»[10].

[Rz 49] *Then is «Privacy» a Defined or an Implied Right?* Under the foregoing circumstances: we are (1) unable to define a specific protected entity of Personal Data, and (2) we face the unquestioned existence of a seemingly unlimited area of «freedom of expression». This often leads to those who have something to gain by attempting to promote unprotected access to Personal Data favorable to their own businesses alleging new community standards and declaring «Privacy does not exist anymore». That kind of language is only useful to promote the notion that, if you can obtain our Personal Data, legally, you can either «report» it or make any other business use of it you like.

[Rz 50] Yet, that may be too hasty a conclusion. We cannot ignore the countervailing constitutional protections arising from the Fourth, the Fifth, and the Sixth Amendments, in criminal procedure matters referred to above, and the civil law legal protections against unlawful acquisition or use of «Personal Data»: in *breach of trust* or of *confidentiality*; against untruthful or *defamatory allegations*; and in *Invasion of Privacy*. This also ignores the importance of the pressure to create *protected areas of «personal choice»* as, for example, in recognition of a right to seek abortion prior to viability[11] and freedom of *access to knowledge of and means of birth control*[12].

[Rz 51] *Personal Data in the EU and the Commonwealth*: The situation is somewhat more favorable to a firm concept of «Personal Data» in the Commonwealth countries and the European Union, today. There are equivalents in those countries for the American constitutional protections. Furthermore, assuming they can hold their own against the onslaught of internet globalization, the EU Data Protection Directive, 95/46/EC obliges all member states of the EU to enact laws for the protection of «Personal Data».

> Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data.... «[Personal data» shall mean any information relating to an identified or identifiable natural person

9 Mr. Justice Holmes in Schenck v. United States, 1918.

10 In Brandenburg v. Ohio, 1969.

11 Roe v. Wade, 1973.

12 Griswold v. Connecticut, 1965.

(«data subject»).[13]

[Rz 52] Unfortunately, when it comes to actually processing «Personal Data», far too often that is in the hands of the same financial institutions and «Personal Data» collection businesses in the United States, that have created the problems for America.

[Rz 53] The abuse of «Personal Data» dossiers in the dictatorships of the 20th century is still a live memory in Europe. In the words of Joachim Gauck, President of the German Federal Republic, who won the affection of the German people as an open dissenter in the days of the former communist regime in East Germany, and later as Commissioner for the captured Files of the Former East German Secret Police (the STASI):

> The Ministry of State Security influenced career rise or fall, took advantage of human weaknesses, and did not hesitate to intrude into the private sphere of its victims and to utilize the most intimate information for its own purposes. Medical confidentiality, bank and postal secrecy, the inviolability of home life, even the basic rights of the citizen laid down in the Constitution of the German Democratic Republic did not pose a limit in the minds of these people.

[Rz 54] Therefore, with living memory of the abuses of human dignity by the dictatorships of the 20th century, and current efforts to create a realm of protection for «Personal Data» in the European Union, those countries might be much better off in this battle. Unfortunately, those countries also rely heavily on financial and other «Personal Data» gathering institutions headquartered in the United States. The result is, therefore, that **between globalization, and reliance on American business data processors, Europeans are also giving away their hard won «Personal Data» protection systems.**

7 Fear of a Coming «Information Society» and Development of a «Code of Fair Information Practices»

[Rz 55] *Fear of a «Big Brother» State*: If the object of social policy were to create a central file on everybody, then every country could establish its own version of the STASI files. In the wake of the Second World War, that was the first thing that policy-makers in the liberal democratic countries wanted to avoid. The memory of Nazi terror in Germany and the various secret police organizations in the Soviet Union and its satellites were well known and feared, also in the United States. Computerization of all government files was still a distant dream – or a nightmare – depending on whether you dreamt in terms of the aesthetic fluidity of a world of automated «Personal Data» search, or of foreboding of the coming big brother state.

[Rz 56] *A Future «Code of Fair Information Practices»*: Fears of manipulation in a future «Information Society» had a slight upper hand in policy-makers thinking in the 1960s and 70s. In 1973 the U.S. Department of Health Education and Welfare (HEW) published a report recommending that Congress adopt a «Code of Fair Information Practices». That proposal became a model for legislation both in the United States and in all liberal democratic jurisdictions today. It called for data protection on the following principles:

- The government must not maintain a personal data system, the very existence of which is

[13] EU Data Protection Directive, 95/46/EC: Art. 1 (2); Art. 2 (a).

secret;
- An individual must have access to any information maintained on him or her and be able to learn how it is to be used;
- Information collected for one purpose must not be used for another without the consent of the individual concerned;
- It must be possible to correct or amend an inaccurate file;
- Any agency creating, maintaining, or using personal data files must ensure the accuracy of such files, and their use only for the intended purposes, along with measures to prevent their misuse.[14]

[Rz 57] «*Big Business*» *Was Our Friend*: As already observed, these principles are affirmed in one way or another in all the liberal democratic jurisdictions, today, as far as action by the state is concerned. On the other hand, not only as the result of terrorist threats to our way of life in recent years, but also **because of developing business opportunities to exploit Personal Data, every one of these principles is ignored or breached by private sector agencies that operate on the basis of absence of comprehensive «Personal Data» law in the United States, and the assumption that what is good for the Personal Data business is good for the rest of us.**

[Rz 58] The European Union and Commonwealth countries that have enacted stricter laws fool themselves when they think they are immune from the same abuses as the United States, when they hire Personal Data processing agencies headquartered in the United States, or when they adopt the same take-it-or-leave-it contract «Terms and Conditions» as American financial and other institutions. **Whether «Personal Data» is initially received in countries with more extensive data protection laws or not, if «Personal Data» is later *stored* in the United States the original «Personal Data» protection is lost. Furthermore, globalization through the internet spreads the abuse much further, throwing the veil of unread or unreadable «Terms and Conditions» over the use of internet and computer operations.**

8 From «Fair Information Practices – To Waiving Our Rigths»

8.1 The Short Life of the «Consumer Protection Movement»

[Rz 59] *Implementing the «Code of Fair Information Practices»:* Enough of the chief elements of the proposed «Code of Fair Information Practices» was enacted even in the United States, that those of us alert to the importance of Fair Information Practices, and willing to defend their rights, could have resisted the onrush of abuses in this area. The Privacy Act of 1974 attempted to implement the proposed «Code» in limited, but important ways that, in their avoidance, establish the pattern of abuse of «Personal Data» files in the United States. The most significant first measure was to attempt to keep information collected for one purpose from biasing other relationships with Government:

> No agency [of the federal Government] shall disclose any record which is contained in a system of records... to another agency except pursuant to... prior written [request or] consent of the individual to whom the record pertains, unless disclosure of the record would be... for a

[14] HEW, *Records, Computers, and the Rights of Citizens*,MIT, 1973.

routine use as defined.[15]

[Rz 60] «Routine uses» include, e.g., law enforcement or collection of debts owed to the Government – so never let it be said that Government agencies were ever blind to essential Governmental concerns.

[Rz 61] This provision makes perfectly good sense to «individualistic liberals» – that is to those persons who are ready to supply personal information to government agencies when there is a specific need for such information and it will be applied for that purpose only. Unfortunately, the same provision is incomprehensible to those who believe that «protection of society» itself depends upon the collection and consolidation of as much personal data as possible – with as little disclosure or access as is necessary, regardless of whether any particular threat or purpose exists for such secrecy or not.

[Rz 62] The information technology industry arising at that time also saw the existence of agency personal data files available for consolidation as a business opportunity, whether for government or private sector purposes. Accordingly, wherever we deal with the personal data collection industry we are obliged to waive rights arising under the Privacy Act.

[Rz 63] Nor did passage of the Privacy Act put an end to the drive in Congress and Government agencies to probe the personal background of Government employees and contractors, leading them to outsource such searches to private sector «consumer reporting» or «recruitment assessment agencies», which, precisely because such organizations rely on compiled data (and «data assessment»), requires that applicants waive all Government agency «Personal Data» «Privacy Act» provisions.

[Rz 64] The principle prevailed in the Privacy Act that what may concern one agency, does not have to concern another. For example, an orphan, or one-time welfare recipient, or former juvenile delinquent, or a victim of disaster, did not to have to re-open old wounds when he or she was considered for honors or for employment in later life.

[Rz 65] But **this would become directly at odds with the lifetime assessment product of «background checking» or «recruitment screening agencies». A professional person can generally name peers or mentors who can evaluate his or her performance or achievements over a lifetime. For data collection agencies, «background» is a matter of credit rating, driving record, academic achievement scores, and contacts with public and private sector agencies (as if that were not a private right).**

[Rz 66] *Submitting Our Own Personal Information vs. Third Party Collection*: There is no honest «Personal Data», that, if properly authenticated, cannot be given to or come from the data subject him or herself (even allowing for the exception that some very limited personal medical information could cause undue distress). This principle was accordingly adopted in the Privacy Act of 1974 governing «Personal Data» in U.S. Government files:

> Each agency... shall... collect information to the greatest extent practicable directly from the subject individual...[16].

[Rz 67] *Personal References vs. the «Referencing» Business*: Personal references are a matter of opinion. No one has an obligation to recommend anyone else. On the other hand, agreeing to give

15 Privacy Act, 5 USC §552a.

16 Privacy Act, 5 USC §552a (e)(2).

a reference amounts to an indication that the writer is willing to support the candidate in some way. Confidentiality of references is, therefore, something that exists largely because employers and admission committees tend to regard them as more secure, honest, or revealing. However, the possibility that some confidential references may sometimes be biased against the person seeking support was long ago acknowledged by the U.S. Congress, leading to the provision in the Family Educational Rights and Privacy Act (FERPA) leaving the choice of whether a student or graduate should allow his or her reference file to remain confidential or not to the individual.

[Rz 68] And what have we lost by that? The geniuses in our schools and universities are not likely to suffer whatever they do. However, after 12 or 16 years of schooling and higher education, those of us who are not so distinguished also have a right to know how our schools and universities assess, and substantiate their assessment of what we have accomplished or what we have not achieved but could have. **There is no such thing as a right to squelch your students or graduates in silence.**

[Rz 69] «Recruitment screening agencies» that say they «*verify* high school graduation and your highest degrees earned» do not simply seek authenticated copies of your degrees and certificates for this purpose. Instead, they demand a «waiver» of the FERPA, the U.S. law that guaranties the privacy of our school and university student files. (Again, there are comparable laws in common law and EU jurisdictions, not for the openness of references, but for protecting the «Privacy» of files.) **For many reasons it is not a good idea to comply with a demand for complete waiver – or, by extension, not to choose such an employer. By allowing personal data collection agencies to «evaluate» files consisting of mixed records of testing and random notes of all the clerks and officials who have had access to a file, you give up the expectation of personal knowledge of the achievements and performance of the applicant, and permit a statistical or impressionistic assessment of what may be only gossip and hearsay.**

[Rz 70] Every student knows that school and university files contain much more than just your grades (and date of graduation which EEO employers should, by law, not be looking for). They also include academic and psychological testing and counseling results, certain medical records, school discipline reports, comments by teachers or professors who think highly of you and of those who don't, and more. All of that effort was collected originally to promote student development – not to allow outsiders to come in to pick out what for them are fixed lifelong scores. Therefore, sign one of these FERPA «waivers» and you allow «*search and seizure of your files without a warrant*» possibly to your own detriment though you will never know for what.

[Rz 71] *Dependent Status vs. Employee Right-to-Know*: The danger of exploitation of dependent status of employees has also been widely recognized leading to «employee right-to-know laws» in a number of U.S. states, giving employees and former employees the right of access to their own personnel files. Human resources organizations have pushed back with enactment of so-called «good faith reference laws» that would protect employer personnel offices from liability in going after «disruptive» former employees. Those remarks are not «references» in any accepted sense.

[Rz 72] **The First Amendment gives former employers (or their personnel offices) the right to say what they please about a person, so long as it is in fact «truthful», «in good faith», and «not malicious». This should never lead to the conclusion that one cannot report substantiated wrongdoing. But it may also be illegal merely to attempt to prevent a person's legitimate opportunity of future employment**.

9 From «Collecting and Transmitting Credit Information», To Assessing «Attitude, Motivation, and Behaviour»

[Rz 73] ***From:*** *«Consumer Protection»*, ***To:*** *«Consumer Psycho-Analytics»:* The «Personal Data» collection industry in the United States began long before Social Media as «credit reporting» or «tracking» of regularity of repayment by borrowers. «Credit reporting» was never simply factual, and often included remarks on character and reputation. To the collection agent mentality delay in, or failure to make timely repayment, regardless of for what reason, is equivalent to immorality. Not much thought is lost on scout's «duty, honor, country». Stereotyping and other abuses were common, in the still unregulated industry. «Red-lining», the practice by banks and other financial institutions of drawing red lines around deteriorated and minority areas, where they did not choose to lend, was widely suspected by the late 1960s. Members of the «Consumer Protection Movement» in Congress were determined to eliminate barriers to lending in central urban areas, and passage of the Fair Credit Reporting Act (FCRA) of 1970 is attributed to their efforts.

[Rz 74] **Members of the «Consumer Protection Movement» were surely also aware of the dangers of profiling and maintaining dossiers on less favored members of society in the dictatorships of the early part of the century. Yet, they appear to have made a deal in inching toward regulation of «credit reporting» practices, whereby the industry managed to get «credit» based measurement of «character» and «reputation» into the preamble of the FCRA:**

> An elaborate mechanism has been developed for investigating and evaluating the *credit worthiness, credit standing, credit capacity, character, and general reputation* of consumers[17] (Italics added.)

[Rz 75] There is far more in the FCRA than the preamble, however. And the courts are able to find ample evidence of legislative intent that «credit reporting» should be «fair and equitable to the consumer». See, for example:

> The FCRA was enacted in order to ensure that consumer reporting agencies adopt reasonable procedures for meeting the needs of commerce for consumer credit, personnel, insurance and other information in a manner which is *fair and equitable to the consumer, with regard to the confidentiality, accuracy, relevancy, and proper utilization of such information*[18] (Italics added).

[Rz 76] The «credit bureaus», as they were then known («Consumer Reporting Agencies» or CRAs in the current law) were already promoting their «credit reports» as measures of suitability for employment in the early days. That desire for automatic selection scoring criteria is even more widespread today among those HR persons who have difficulty in assessing qualitative achievement. The HR Handbook of Norfolk State University in Virginia is a classic example in the prominence it gives «credit reports» in the hiring process:

> ... The decision to offer employment will be based on the following review of the individual's credit check: (1.) That an individual is current with paying their financial obligations. (2.) Bankruptcies in one's credit background cannot be used to determine eligibility for employment as per the FCRA. [It is also prohibited by U.S. bankruptcy law.] (3.) The number of overdue obligations will be reviewed. (4.) Extenuating circumstances as put forth by the applicant, for the delinquency in paying obligations will be taken into account. If the results

[17] FCRA, 15 USC 1681a (2).

[18] [3rd Cir. 1997], with many similar citations.

> of the credit check are negative, the University must inform the applicant that it plans on taking adverse action....

[Rz 77] **In university life, particularly, we like to see greater regard for our academic and professional accomplishments and less concentration on how much our financial situation after years in the academic proletariat shows we just need a job.** (75% of faculty in American colleges and universities, today, teach in part-time or adjunct positions, and, therefore, may spend many years at or below the legal minimum wage.)

[Rz 78] Clearly many in Congress, apparently with little resistance from the public, had been persuaded of the importance of «credit reporting» as the basis of character judgment. It was 30-some years since the Great Depression. Memory was not very good, especially in good economic times. «Credit reporting» was treated as factual reporting. The FCRA provided the mechanism for seeking correction of errors. So there was little resistance to the CRAs judging character on the basis of «credit reporting»:

> o consumer may bring any action or proceeding in the nature of defamation, invasion of privacy, or negligence with respect to the reporting of information against any consumer reporting agency, any user or information, or person who furnishes information to a consumer reporting agency, based on information disclosed...[19].

[Rz 79] This may sound acceptable as long as we are talking about verifiable reports from creditors. Yet, while this special protection was presumably intended for facts and figures «Consumer Reports» (the old «credit reports»), the same provision also applies to the so-called «Investigative Consumer Report». **If you consent to an «Investigative Consumer Report» on your «character, reputation, and lifestyle [whatever that is]» the provision above amounts to statutory deprivation of the protections of the Fourth, the Fifth, and the Sixth Amendments to the Constitution of the United States – notably the right to know the nature of an accusation and the right to confront witnesses.**

[Rz 80] In 1970 there was still little inkling of the coming IT revolution. The Privacy Act was still five years down the road. The business «resume» had only recently been invented. And far from today's personal data matching services the business pitch of detecting «*lying on resumes*», and the danger of the CRA invented concept of «*negligent hiring*» for failure to buy the new CRA product, the «Investigative Consumer Report» was far in the future. Business school emphasis was on creative representation of the business career path. **Has business writing become more misleading over the years? You only have to look at what is hidden in, say, the 25 or more pages of «Terms & Conditions» of the various «End User Licensing Agreements» (EULAS) on the internet, subject to revision at any time, where we are told to keep abreast of changes ourselves to deal with online providers, to answer that question.**

[Rz 81] In the 1980s, the electric typewriter was still the dominant IT medium. The criminal records bureaus could hardly have been computerized before the turn of the millennium. Only at the point at which computer searches could access public records – and if «privacy waiver» were obtained – access school and university records as well, could a meaningful new IT-«Personal Data» product emerge. This history tells us a great deal, however. **The «Personal Data» collection industry (largely of «recruitment screening» agencies descended from the original CRAs),**

[19] FCRA, 15 USC §1681h(e).

unlike the dot com boom, did not make any new or valuable contribution to the economy. It merely provided a more efficient means of accessing and processing information that we already possessed.

[Rz 82] The FCRA today, as amended, provides not only for the «Consumer Report», the old «credit report» by another name, but also the «Investigative Consumer Report», which by statute should not include «credit reporting», but instead relies on «interviews» with your «friends, neighbors, and associates» to gather information on your «character, general reputation, and lifestyle (undefined but presumed in the literature to mean sex life although that would be illegal if said directly)». **If you were asked to provide references to character and professional ability, but would not name those «friends, neighbors, and associates» as your first choices, then hesitancy to consent to such a skewed «background check» is obvious.**

[Rz 83] The FCRA requires that an employer that demands an «Investigative Consumer Report» provide «clear and conspicuous» notice on a separate sheet from its application form detailing the nature of such an investigation and obtain a signed consent. While you can, of course, refuse to consent, in the world of take-it-or-leave-it online applications, you have no real choice. Non-employment related requests do not require the detailed notice and consent, but essentially leave less choice:

> his report will include character, general reputation, personal characteristics, mode of living, work habits, performance, experience, along with reasons for termination of past employment... obtained through personal interviews with associates who have knowledge concerning such items of information[20].

[Rz 84] The trouble with this standard of efficiency is still less what the product purports to be, though that is intrusive enough, but rather the standards of accuracy and security involved in its production.

[Rz 85] Yes, the IT and computers that process the work are more efficient than they used to be. But we hear that those that do the research and the interviews, are: «part-time truck drivers, retired persons, homemakers, and small business people»[21] who hire on for spare-time work doing telephone interviews of your «friends, neighbors, and associates». Maybe these part-time interviewers are all good citizens who need to add to their incomes. Perhaps you would have confidence in them to sit as a jury of your peers if you were trying a case where they had to apply common sense and practical experience to judge guilt or innocence in a traffic accident. But, **if it were up to you, wouldn't you choose a more qualified panel to do profile interviews on your «character, reputation, and mode of living» – where you know that they also have to balance positive and negative attributes to satisfy their agency managers?**

[Rz 86] *Criminal Records Bureau Checking*: Criminal records bureaus may or may not be computerized today. But. **you are much better off to apply for a records check yourself, and have it sent to your employer – only after you verify that the file, or no-file record, has your own name on it and is not a mis-match.** Your school or college registrar is happy to send out verification of graduation at your request. But, do you really want to throw in teacher/counselor comments back to grammar school, which you will do if you release all that with a waiver of FERPA? **Doubtless there is someone you would choose to write a school or college reference, or a job skill re-**

[20] Colgate University, «Notification and Authorization to Obtain Information».

[21] Federal Trade Commission staff opinion letter, «the LeBlanc letter», June 9, 1998.

port, rather than your hi-bye «friends, neighbors, and associates». It's a question of whether you think that they all disregard private ambition, personal rivalry, or petty grievances, when they agree to consult with strangers on an investigative report that will determine your job future.

[Rz 87] *What Happens to Old «Background Checks»?* Finally, once you have gone through such an out-sourced «recruitment screening agency» process, do you really want that agency to continue sending out that file to any CRA customer who turns up with a «legitimate business purpose»? **Maybe you think that you can not say «no» to application «waivers». But, don't you think we all could, if we all did, at the same time?**

[Rz 88] *Placement and «Psycho-Analytics»:* Suppose you do consent to an «Investigative Consumer Report». Suppose you do waive FERPA and consent to release of your school and university files. Suppose those perfectly respectable part-timers do interview your «friends, neighbors, and associates». Do you think that the billion-dollar companies behind those operations are merely going to send your graduate admissions office or your prospective employer the same thing that you would expect from your college mentor or senior professional supervisor? Look closely and you will find that that is not even what they are looking for:

> People rarely succeed or fail due to lack of skills or intelligence. Instead their success or failure is due to personal characteristics such as attitude, motivation, and temperament (behavior).... InfoLink has partnered with a company which provides the best product on the market to analyze the behavioral requirements for any position. This program enables you and your associates to quickly reach consensus on the real demands of the job. (A «Recruitment Screening» CRA on itself)

[Rz 89] Maybe your university or your employer or even you yourself are completely persuaded of the reliability of the Psycho-Analytical reliability in obtaining a true profile of yourself by going back as far as your grammar school files and drawing on the impressions of «friends, neighbors, and associates». Is that what you are applying to graduate school for, or applying to this new employer for? Are you looking backward to what you were in school or college or do you have some expectation from graduate study or professional employment that you want to achieve regardless of what your psycho-social profile was in school or college days.

[Rz 90] **This kind of Psycho-Analytical profiling is not the result of overreaching by the NSA, or of runaway surveillance by government authorities – we presume that that «recruitment screening agency» is looking for real «Big Data» for «national security» purposes. But, in these personal business dealings we face the oldest flaw in the IT revolution: «*Garbage in – Garbage out*».**

[Rz 91] «*Legitimate Business Interest*» – *the Right to Spy On People*: Under the FCRA, those who have a «*legitimate business interest*» are also able to seek what amounts to pure gossip and hearsay about us. Many distinguished colleges and universities, many large employers, and a host of purely commercial entities, now ask for a «*consumer report*», or a more comprehensive – though more questionable – «*investigative consumer report*», for admissions, hiring, new account opening, etc. By law, employers must inform you – employers must also provide this information on a separate sheet from the rest of the application and obtain your signature confirming that you have understood the request. The FCRA is not as scrupulous with regard to others. And there is nothing to deter a CRA once it has collected your personal data from re-selling it to anyone who declares «*a legitimate business interest*». **These files are not just for one particular transaction.**

Once we sign, we have also «waived» our «*right against double jeopardy*». The background file can be sold over and over again.

[Rz 92] *Some Comparative Law Thoughts on Asking «Lifestyle» and Sexual Identity*: It is illegal «to consider» most sex life references in credit, admissions, and employment matters in the United States today. «Not consider» means «not to ask» in the U.S. – but «mode of living» and «lifestyle» are euphemisms that still get by.

[Rz 93] In the U.K., it is also illegal «to consider» legally protected sexual identity matters. However, Equal Employment practices differ there. In order «not to consider» sexual identity, the practice has arisen for human resources offices to collect self-designation data for sexual identity, religion, and ethnic/racial origin, presumably to demonstrate non-exclusion or reasonably proportional access. Presumably this would require first establishing the demographic distribution of applicants, and then the presumable proper distribution of employees.

[Rz 94] On the one hand it is quite remarkable that multiculturalism could have taken such a hold in the home country of a former colonial empire that it would attribute such importance to achieving an ethnic, religious, sexual identity distribution in every employer institution. On the other, isn't this an awfully casual way of saying that HR policy either utterly disregards the fact that there are native peoples in the British Isles whose job interests can be disregarded simply for statistical distribution reasons, or that demographic considerations trump, regardless of professional qualifications? It is hard to believe that either of these policies can or should be pursued**. Yet if there is no possibility of the latter, then there is not much purpose in collecting irrelevant personal data to gratify the demographic distribution aspirations of the former.**

[Rz 95] In the U.S. hiring on this basis might itself be considered favoring or disfavoring particular demographic groups, whether for legitimate, or not so legitimate reasons. **The philosophy of those collecting personal data «not to be considered» through the same IT channels employed for personal data «to be considered» on the assumption that there is some benefit accruing to those contributing such data, and that it is kept away from hiring decision-makers, is in a way the same persuasion as that of the major players of the personal data collection industry. It is like climbing Everest. You collect irrelevant «Personal Data» not because there is an overriding need or purpose. It is collected simply because it is there.**

[Rz 96] *Security of Personal Data Databases*: Despite best intentions, an HR database for one purpose is no more secure than a database for another purpose, and data files processed by «recruitment screening agencies», which tend to be located in the United States, where the personal data collection industry and financial institutions have long resisted any such strict personal data protection laws as exist in the U.K., makes a mockery of U.K. personal data protection for hiring purposes.

[Rz 97] Typically a U.K. HR webpage will read, as for example the webpages of a certain North of England university:

> Irrespective of where the data may be [in our system], we will abide by the U.K. Data Protection Act.

[Rz 98] That should mean that their data security is as good as it gets. However, the same paragraph adds tangentially:

> Your information may be controlled and processed by any of our offices. You acknowledge and agree that the location of our offices may change from time to time and that we may acquire other offices in any number of other countries or territories at any time, any one or more of which may act as a controller of and/or process your information.

[Rz 99] It is amazing how many U.K. universities now claim such overseas locations. But, the line continues:

> We will not disclose your data to any other third party *unless for recruitment purposes*... (italics added).

[Rz 100] Now how exactly does all that qualification shade the meaning? «Your information may be controlled and processed by any or our offices.» Really? When we are applying for a vacancy in the only known offices of one of Britain's red-brick local universities in a Manchester suburb? And, «We may acquire other offices in any number of other countries»? Suppose they do open such offices in «other countries», is it likely that expressly the HR files for the North of England area will be filed so far removed from the departments with the vacancies applied for?

[Rz 101] Then, we do come closer to sensible meaning below: a third party may be involved for «recruitment purposes»? In plain English that sounds like outsourcing to a «recruitment screening agency» most of which are American institutions that store data files in the United States, where there is as good as no personal data protection law, and where personal data «assessed» or «evaluated» for one client falls, for that purpose, under the copyright of that agency, and can easily be re-sold to another client. Not every employer, financial institution, or what have you, in the United States will confirm this, but one that does tells us that if a consumer report is obtained,

> The consumer reporting agency may keep a copy of the report and disclose it to others having a legitimate need for such information[22].

[Rz 102] The «legitimate need» language derives from the FCRA – where it originally meant sharing «credit reporting» records with a prospective creditor, not a wholly unrelated prospective employer, who had not made «clear and conspicuous disclosure» to the prospective employment applicant. However, this makes clear that **stored data for re-release is not limited to hard data credit reporting figures anymore. «Assessment» and «evaluation», that the data subject never sees, is for good or bad reported in complete disregard of Fourth Amendment protection against seizure of protected personal data without warrant, Sixth Amendment guaranties of confrontation of witnesses, and Fifth Amendment protection of due process. Furthermore, Personal Data once «assessed» or «evaluated» is not Personal Data anymore. It has become the copyrighted work product of the data collection agency. Thus Personal Data, once disclosed, has lost any protection it may have had. But the personal profile produced by the CRA or «recruitment assessment» agency is protected intellectual property.**

10 Conclusion – Technology and Shady English

[Rz 103] *The purpose of Business School English today* is not so much to inform as (1) to capture the «consumer»: «Listen carefully, our menu has changed», and (2) to escape liability: «Terms & Conditions» are classic examples of how to hide what no one in a bargained-for contract would agree to. Where technology takes over it is not to facilitate «interactivity» or «intercommunication», but to avoid it. The loudspeaker all over again.

[Rz 104] We often hear from IT or Social Media operators that «*Privacy*» does not exist anymore.

[22] RiverSource Insurers of Ameriprise Financial.

They really mean that they do not want to be bound by «*Privacy law*». They tell us that technology has moved *beyond copyright law*, and they should not be bound by copyright either (in this case copyright of media works). Then their special interest organizations promote something like the monster U.S. Digital Millenium Copyright Act (DMCA), that creates statutory dilemmas never dreamt of before. What these people tell us is of course what suits their purposes. The common law itself goes on as before – while they attempt to enforce the more favorable, much more wide-ranging Digital Millenium Copyright Act.

[Rz 105] What is true is not that the «old law» does not exist anymore. Rather, we have to look at the law in context, and update and add new law where necessary. «*Privacy law*» in the United States is alive and well on the books, and many of us would fight to keep it. However, it derives by implication from sources where the word «*Privacy*» itself does not appear. We say that we are protecting «*Privacy*» when we say that the police need a judicial warrant prior for search and seizure. «*Privacy*» is also the implied right protected in reproductive areas. «*Copyright*» is, however, entirely statutory. It is provided for in Article I of the U.S. Constitution, but length of copyright protection has been determined and varied by Congress entirely dependent on influences at work in the legislative area at any given time.

[Rz 106] Changes and advances in «*Privacy*» and «*copyright*» law insofar as the rights of individuals are concerned have come to the Commonwealth and European Union countries – perhaps on the basis of inspiration of early Anglo-American individualistic liberalism, but they are long since a liberalism maturing in the EU and suppressed by commercial special interests in the United States.

[Rz 107] In the United States, advocates of First Amendment «*freedom of speech*» are still fighting the intellectual battles of the 18th century – as if we were still emerging from fear of being cited for sedition against the king. Therefore, because the «Privacy» interest that is protected in the Fourth, the Fifth, and the Sixth Amendments is never named, extremist defenders of the «*right to say anything whatsoever*» (which never existed historically, and certainly never existed in law) always see a conflict with the First Amendment. The EU countries that have had the benefit of U.S. Constitutional historical experience have written more narrow «*freedom of speech*» laws and also attempted to protect personal «*Privacy*» by statute. Similarly, in the EU, «*copyright law*» applies to published or original works. But «*personal data*» is given specific protection as well in separate statutes.

[Rz 108] «*Market Analytics*» *and* «*Recruitment Screening*»: There are two separate commercial forces at work in the attack on «*Personal Data*». The one seeking to collect our «Personal Data» *to market to us* («*market analytics*»). The other, seeking to collect our «Personal Data» *to market us* ourselves («*recruitment screening*»). Both of these *marketing techniques* are highly profitable, but neither one of them adds anything new to the economy.

[Rz 109] *Information Technology*, IT, and the so-called «*Social Media*», do add new technical advances. However, while developers and entrepreneurs may become immensely wealthy from these advances, the public itself, the users of this technology are often unscrupulously exploited.

[Rz 110] **What the philosophers of *the internet* have conspicuously overlooked in all of this is the question: «*Who owns the internet*?» Even if the IT and the social media are distributed free, *access to the internet* itself has become an expense often well beyond the means of those to whom it was supposed to be the greatest benefit: the young, the elderly, and the disadvantaged of society.**

This paper was prepared for discussion at the «Symposium on Social Media, Big Data and Cloud: Trends and Issues in Asia,» HKUST-Nie Social Media Lab, Hong Kong, 3 October, 2013, http://smedia.ust.hk/events/bigdata. The authors are grateful to Rafael Chodos and Wild Chang, attorneys in Los Angeles, for reviewing the drafts.

Orlan Lee, M.A., Dr..Jur., JurisDr., LL.M., is a Visiting Fellow/Life Member of Clare Hall, a College for Advanced Study in the University of Cambridge. He has been variously Associate Professor of East Asian Studies at Washington University, St. Louis; Adjunct Professor of Business and Management at the Hong Kong University of Science & Technology; and Professor of Management at the New York Institute of Technology. His recent book, Waiving Our Rights, is concerned with mandatory waiver of our fundamental rights in what should be ordinary business transactions.

James She, M.Sc., Ph.D., is Assistant Professor of Electronic and Computer Engineering at the Hong Kong University of Science & Technology, and Research Fellow in the Computer Lab, at the University of Cambridge. He is Founding Director of Asia's first social media lab, HKUST-Nie Social Media Lab, where he spearheads multidisciplinary research and innovation in cyber-physical social media systems, viral media analytics, and mobile media broadcast H systems. He is a member of the World Economic Forum's Global Agenda Council (Social Media).