Chicago-Kent Law Review

Volume 84
Issue 3 *Symposium: Data Devolution: Corporate Information Security, Consumers, and the Future of Regulation*

Article 7

June 2009

Returning to a Principled Basis for Data Protection

Gus Hosein

RETURNING TO A PRINCIPLED BASIS FOR DATA PROTECTION

GUS HOSEIN*

INTRODUCTION

We frequently hear that privacy and security or civil liberties and security are a trade-off—that they are bounded by one another.[1] A common response to this assertion is citing the quotation from Benjamin Franklin that those who give up liberty for security deserve neither. Surely we can generate a more thoughtful response than this. Balance is a very simplistic notion. It is not just security at stake versus individual liberties, and we must do more than just seek to be both safe and free. There is much more at stake. However, frequently when we try to do better, we actually seem to drop out the discussion of underlying principles.[2]

I. FORGETTING PRINCIPLES AND FOCUSING ON COSTS

Changes in commercial products based on government policy have been prevalent recently. For example, data retention policies compel Internet service providers (ISP's) and telephone companies to retain the data[3] they have on consumers such as the logs of telephone calls and e-mails sent and received. When governments propose this policy they sound very reasonable. They say, "Look, we need this, it is absolutely necessary to combat terror threats; we understand this issue of privacy but we really need to focus on more important issues. Just for now, we must balance privacy away." And what do we say in return? We say these actions are very inva-

* Dr. Gus Hosein is a Visiting Senior Fellow at the London School of Economics in the Information Systems and Innovation Group in the Department of Management.

1. For a discussion of the alleged tradeoffs of security and privacy see, for example, Candice L. Kline, *Security Theater And Database-Driven,* 39 U. TOL. L. REV. 443 (2008); Daniel J. Solove, *Data Mining And The Security-Liberty Debate,* 75 U. CHI. L. REV. 343 (2008).

2. For a discussion of principles-based analysis see, for example, Melissa Harrison, *The Evolution Of Montana's Privacy-Enhanced Search And Seizure Analysis: A Return To First Principles,* 64 MONT. L. REV. 245 (2003).

3. For a discussion of data retention, see, for example, Francesca Bignami, *Privacy And Law Enforcement In The European Union: The Data Retention Directive,* 8 CHI. J. INT'L L. 233 (2007); Caspar Bowden, *Closed Circuit Television For Inside Your Head: Blanket Traffic Data Retention And The Emergency Anti-Terrorism Legislation,* 2002 DUKE L. & TECH. REV. 5 (2002); Catherine Crump, *Data Retention: Privacy, Anonymity, And Accountability Online* 56 STAN. L. REV. 191 (2003).

sive and illegal under either the constitution of country X, or the European Convention of Human Rights.[4]

As privacy advocates we have also become expert at public policy analysis. We therefore sometimes go a little further and point out that retention as a policy is very costly for telephone companies and ISPs, thereby attaching a profit-oriented concern. Companies say privacy-invasive[5] tactics are going to be costly. In turn, the cost is going to be imposed on the consumer. Consequently, the debate quickly moves to focus on the costs of the policy.

For instance, when privacy advocates took on the data retention policy in the European Union, we argued that data retention invades the privacy of Europeans, that it is illegal under the European Convention on Human Rights, threatens consumer confidence, burdens European industry, and will require even more invasive laws to make it work. Too often, however, the only argument that people listen to is that it is going to be costly.

A. The Third Body Problem: Industry

The cycle of these stories are quite typical: bad policy is proposed, civil libertarians complain about privacy, get some attention but not much, and policy moves forward nonetheless. So we then resort to other methods and generate more concern and broader coalitions.

One prime example of this is travel surveillance. Countries around the world are establishing legal and technological requirements to gain access to passenger data for domestic flights using the rationale of combating terrorism.[6] Civil Libertarians step in and argue that these approaches are invasive because if you look at what programs plan on doing with this data,

4. For a discussion of the European Convention of Human Rights, see D.J. HARRIS, M. O'BOYLE & C. WARBRICK, LAW OF THE EUROPEAN UNION 283–301 (1995). For jurisprudence on Article 8, please see Douwe Korff, The Standard Approch Under Articles 8-11 ECHR and Article 2 ECHR, Presentation Before at the European Commission Justice and Home Affairs Conference (May 19–20, 2009).

5. For a discussion of privacy invasion, see, for example, Daniel Gomez-Sanchez, *Copyright Law, Privacy, And Illegal File Sharing: Defeating A Defendant's Claims Of Privacy Invasion,* 24 TOURO L. REV. 73 (2008); Daniel P. O'Gorman, *Looking Out For Your Employees: Employers' Surreptitious Physical Surveillance Of Employees And The Tort Of Invasion Of Privacy,* 85 NEB. L. REV. 212 (2006).

6. For a discussion of passenger data, see, for example, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-06-374T, AVIATION SECURITY: SIGNIFICANT MANAGEMENT CHALLENGES MAY ADVERSELY AFFECT IMPLEMENTATION OF THE TRANSPORTATION SECURITY ADMINISTRATION'S SECURE FLIGHT PROGRAM (2006); SECURE FLIGHT WORKING GROUP, REPORT OF THE SECURE FLIGHT WORKING GROUP (2005), *available at* http://www.epic.org/privacy/airtravel/sfwg_report_091905.pdf; Timothy M. Ravich, *Is Airline Passenger Profiling Necessary?,* 62 U. MIAMI L. REV. 1 (2007); Peter M. Shane, *The Bureaucratic Due Process Of Government Watch Lists,* 75 GEO. WASH. L. REV. 804 (2007).

they plan on analyzing it and profiling citizens.[7] It is hard to get people to care about their personal privacy in the face of the governments' recommendation. But when we also say actions are going to be costly, and that a significant cost to the air carriers will be passed on to consumers, concern grows in both public and political circles. Time and inconvenience also play a role, where people do not want to be subjected to greater delays due to additional security controls, such as early check-ins required due to data processing. In turn, industries may be placed at a competitive disadvantage, like how rules apply differently to travel by air or rail.[8]

The increased cost factor is usually because there is now an intermediary for modern surveillance: the private sector. This often introduces a barrier for a governments' deployment of surveillance policy, but equally, it permits a less accountable deployment of surveillance techniques.

Industry can be called upon to deploy government surveillance in ways that the state is unable to do itself. For those who do not remember the 1990's crypto war days,[9] the Clinton administration was obsessed with trying to make sure we use government-approved security technologies[10] that would allow for back door access to law enforcement.[11] Now we are seeing this discussion replicated in connection with developing intercept capabilities in communication systems including voice over IP.[12] China has ordered various software producers and hardware producers to change

7. For a discussion of profiling, see, for example, Murad Hussain, *Defending The Faithful: Speaking The Language Of Group Harm In Free Exercise Challenges To Counterterrorism Profiling*, 117 YALE L.J. 920 (2008); Ruth Singer, *Race Ipsa? Racial Profiling, Terrorism And The Future*, 1 DEPAUL J. FOR SOC. JUST. 293 (2008).

8. For a discussion of the challenges introduced by security measures to a variety of travel infrastructures, see UK HOME AFFAIRS COMMITTEE THIRD REPORT ON E-BORDERS, HOUSE OF COMMONS (2009).

9. For a discussion of the crypto wars and the Clipper Chip, see, for example, Vandana Pednekar-Magal, *The State And Telecom Surveillance Policy: The Clipper Chip Initiative*, 8 COMM. L. & POL'Y 429 (2003); A. Michael Froomkin, *The Metaphor Is The Key: Cryptography, The Clipper Chip, And The Constitution*, 143 U. PA. L. REV. 709 (1995); Janine S. Hiller, *From Clipper Ships To Clipper Chips: The Evolution Of Payment Systems For Electronic Commerce*, 17 J.L. & COM. 53 (1997).

10. For a discussion of cryptography, see, for example, David Banisar, *Stopping Science: The Case Of Cryptography*, 9 HEALTH MATRIX 253 (1999); Christopher D. Hoffman, *Encrypted Digital Cash Transfers: Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations*, 21 FORDHAM INT'L L.J. 799 (1998); Marcus Maher, *International Protection Of U.S. Law Enforcement Interests In Cryptography*, 5 RICH. J.L. & TECH. 13 (1999).

11. For a discussion of wiretapping capabilities, see, for example, Anuj C. Desai, *Wiretapping Before the Wires: The Post Office and the Birth of Communications Privacy*, 60 STAN. L. REV. 553 (2007).

12. For example, see Testimony of Ms. Laura Parsky, Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, to the Senate Committee on Commerce, Science and Transportation on the VOIP Regulatory Freedom Act, S. 2281, June 16, 2004.

technology in order to allow for surveillance, for example.[13]

Ironically as the relationships between government, citizens, and industry change, governments all argue the same thing: that they are just trying to maintain the status quo. That is, in the face of changing technologies, they contend that what all of their policies are trying to do is to stay on top of these changes. There is very little room for discussion of principle when governments use these convincing ideas from arguments long ago settled. That is, the principle of privacy was considered originally when interception law was established, and rather now the problem in our midst, according to governments, is the mere *modernization* of these policies. Therefore, we are almost compelled to focus our energies on debates regarding feasibility and the challenges to industry. Put another, way, when we start getting into the argument about circumventing the laws, costs and anticompetitive effects, we have already lost the opportunity for the principled debate about whether or not these approaches are a good idea.

B. The Fourth Body: Technology

Moving from a two body problem, which consists of the battle between government needs and individual rights interests, the three body problem of industry's involvement has introduced a further challenge: the role of technology. The introduction of Internet surveillance using the legal regimes for traditional surveillance has significant implications for both human rights and industry, even as governments contend they are merely *modernizing* their powers.

New technologies are often perceived as being progressive as we rarely consider the ramifications of their use on traditional infrastructures. Europeans generally quietly nod when it comes to ID cards,[14] as they imagine their 'cards' are indeed just that: paper, cardboard, or perhaps plastic items containing some information. A *modern* identity card is very much different, however; in fact, a card is not even required. The British Government is in the process of introducing exactly such a card: a plastic card containing a chip and radio-frequency identification to transmit biometric informa-

13. For a discussion of the surveillance of Skype communications in China, see NART VILLENEUVE, BREACHING TRUST: AN ANALYSIS OF SURVEILLANCE AND SECURITY PRACTICES ON CHINA'S TOM-SKYPE PLATFORM: A JOINT REPORT OF THE INFORMATION WARFARE MONITOR AND THE OPEN NET INITIATIVE ASIA (2008). This led to a response from Skype's president, Josh Silverman. Skype President Addresses Chinese Privacy Breach, http://share.skype.com/sites/en/2008/10/skype_president_addresses_chin.html (last visited Nov. 9, 2009).

14. For a discussion of identity cards see, for example, Adrian Beck and Kate Broadhurst, *Policing the Community:The Impact of National Identity Cards in the European Union*, 24 J. ETHNIC & MIGRATION STUD. 413 (1998); Clare Sullivan, *The United Kingdom Identity Cards Act 2006-Civil or Criminal?*, 15 INT'L J.L. & INFO. TECH. 320 (2007).

tion on individuals, and all these data will be stored on a central register. A system of this scale has never been done before. Essentially, they are requiring that a national register database be created with a file on every resident in the United Kingdom with ten fingerprints, face scans, and the like. Every time you open a bank account, every time you cross the border, every time you interact within the public and private spheres, you would be required to be verified against that central database.

There are serious civil liberties concerns, especially with the idea of fingerprinting the entire population. British authorities also intend to use this fingerprint data for verifying against fingerprints at the scene of crimes. As the government was portraying Britain as the only country without ID cards, thus attempting to demonstrate that ID cards were not a gross personal interference, they were concealing the identity system's role as a law enforcement measure. A more Euro-friendly British population wasn't likely to have the same view of identity cards as they have previously held, that is that cards were a *Germanic* concept, evoking memories of Nazi Germany or Communist Europe.[15] As such, we knew we were not going to win the debate based on civil liberties concerns, so we decided to focus on the fact that the system being proposed was unprecedented, highly complex, untested, and required a significant investment.

Experts at the London School of Economics and Political Science wrote a report to analyse the Government's proposals, supported by years of research bringing together expert groups.[16] Although we spent less than 10% of the report focusing on the cost of the government's proposed system, and focused much more on the technological challenges, the likely costs received the bulk of the media coverage and parliamentary attention, and that is when people started to get angry. That is when people started changing their minds about the card, and the support for the policy dropped significantly. So again, this meant that the time for principled debate was over, and we are now just worrying about the practical issue of costs. Even the technological debate was reduced to a discussion of costs rather than feasibility, effectiveness, and the social implications of fingerprinting an entire population. Privacy is thus not the only victim of a simplified public discourse.

15. Former Prime Minister Margaret Thatcher famously attacked ID cards as a 'Germanic' concept. For more information regarding identify cards, see, for example, Rob Hyde & Lena Schlenzka *Identity Crisis Over UK Cards*, TELEGRAPH.CO.UK, Mar. 8, 2005, http://www.telegraph.co.uk/expat/4195483/Identity-crisis-over-UK-cards.html.

16. *See* LSE Identity Project Reports, http://identityproject.lse.ac.uk/#LSE_Identity_Project_Reports (last visited Apr. 1, 2009).

B. *The Future of Principled Privacy Arguments*

Modern laws now implicate many more actors than the citizen and the state. Industry and technology are also affected by policy shifts. Whereas we used to focus on principled debates on whether policy change was necessary or needed, now our policy debates are possibly more pragmatic and focus on costs. Any complexity involving legalities, feasibility or technological uncertainty are more interesting to audiences when they are summarized as costs and economic imbalances. This dumbing-down of public policy debates is troublesome.

If people have nothing to hide, what do they fear? The answer is the cost. This pragmatic approach is spreading toward all these other civil liberties and privacy related policy areas. Has it come to a point where it basically comes down to industry to decide whether or not policy is a good idea based on how easy or challenging it is for them to deploy?

Complex policy questions need to be raised as our policies are becoming more technological, economically, and socially complicated. Yet we are dumbing down our policy processes too often by focusing on costs. We need to return to our traditional public policy analyses that have more multi-faceted approaches.

Most importantly we must assess the roles that technologies will play in the future of policy-making. When we do consider technology, we first look at costs, then at effectiveness, and perhaps eventually at matters of principle. So we ask questions like "do the technologies work?" Even if they do not, we have hope that technologies improve over time. For instance, if we are not going to oppose ID cards on the basis of civil liberty constraints, then perhaps we can focus on asking whether the biometrics work? Early studies indicate that biometrics do not easily work the way we hope, particularly when we imagine deployment at a national scale with 60 to 100 million people with ten fingerprints in the database for day-to-day use.[17] But, then when we point out this pragmatic fact and try to cultivate the debate, people come back saying that the technology will get better.

Even if we question whether the technology will ever truly work, it is merely another distraction away from the principled debate. So while it is highly questionable whether technologies will ever work as perfectly as the policy-makers dream, perhaps we must entertain their imaginative visions for the sake of having a real debate.

17. For a good discussion of biometric challenges, see GENERAL ACCOUNTING OFFICE, CHALLENGES IN USING BIOMETRICS, STATEMENT OF KEITH A RHODES TO THE SUBCOMMITTEE ON TECHNOLOGY, INFORMATION POLICY, INTERGOVERNMENTAL RELATIONS, AND THE CENSUS, COMMITTEE ON GOVERNMENT REFORM, HOUSE OF REPRESENTATIVES (2003).

So let's presume that the technology gets better and these things actually did work. If our closed-circuit television cameras[18] really could recognize your face and whether you are a wanted terrorist, that would be helpful. Does that mean the debate is over? If it really is cost efficient and technologically feasible, our cost benefits are actually measurable. But can and should we really measure it that way? If suddenly ID cards became incredibly cheap tomorrow, does that mean the policy is a good idea?

That is what we are facing if we move to this pragmatic debate. If we implement communications data retention at all communication points globally, with the cost of storage actually decreasing dramatically year to year, the actual cost of implementing communication data retention will fall. Once this cost has declined, does that mean we actually like data retention? Again, if we move into the pragmatic debate as if there are no consequences, we are going to be caught in this technology argument. Often the only other voice in these debates is again industry, and where they choose to fall within these debates will determine the outcome.

The debate must be first about principle, then we can focus on public policy analysis. Approaching it any other way leaves too much to fortune.

18. For a discussion of CCTV, see, for example, Clive Norris & Michael McCahill, *Cctv: Beyond Penal Modernism?*, 46 BRIT. J. CRIMINOLOGY 97 (2006).