Personal Data Privacy and Protection in a Surveillance Era:
Technologies and Practices

Christina Akrivopoulou
Democritus University of Thrace, Greece

Athanasios-Efstratios Psygkas
Yale Law School, USA

Information Science REFERENCE

INFORMATION SCIENCE REFERENCE
Hershey · New York

Director of Editorial Content: Kristin Klinger
Director of Book Publications: Julia Mosemann
Acquisitions Editor: Lindsay Johnston
Development Editor: Michael Killian
Publishing Assistant: Casey Conapitski
Typesetter: Casey Conapitski
Production Editor: Jamie Snavely
Cover Design: Lisa Tosheff

Published in the United States of America by
Information Science Reference (an imprint of IGI Global)
701 E. Chocolate Avenue
Hershey PA 17033
Tel: 717-533-8845
Fax: 717-533-8661
E-mail: cust@igi-global.com
Web site: http://www.igi-global.com

Library of Congress Cataloging-in-Publication Data

Personal data privacy and protection in a survillance era : technologies and practices / Christina Akrivopoulou and Athanasios Psygkas, editors.
p. cm.
Includes bibliographical references and index.
Summary: "This book spans a number of interdependent and emerging topics in the area of legal protection of privacy and technology and explores the new threats that cyberspace poses to the privacy of individuals, as well as the threats that surveillance technologies generate in public spaces and in digital communication"--Provided by publisher.
ISBN 978-1-60960-083-9 (hardcover) -- ISBN 978-1-60960-085-3 (ebook) 1. Data protection--Law and legislation--United States. 2. Electronic surveillance--Law and legislation--United States. 3. Privacy, Right of--United States. 4. Records--Access control--United States. 5. Digital communications--United States. I. Akrivopoulou, Christina. II. Psygkas, Athanasios.
KF1263.C65P47 2011
342.7308'58--dc22
2010033436

British Cataloguing in Publication Data
A Cataloguing in Publication record for this book is available from the British Library.

Chapter 3
Hasta La Vista Privacy, or How Technology Terminated Privacy

Konstantinos K. Stylianou
University of Pennsylvania, USA

ABSTRACT

Lawyers find great joy in pointing out the destructive effects of digital technology on privacy and naturally expect the law to avert overexposure of people's personal information. This essay takes a different view by arguing that the trajectory of technological developments renders the expansive collection of personal data inevitable, and hence the law's primary interest should lie in regulating the use—not the collection—of information. This does not foreshadow the end of privacy, but rather suggests a necessary reconceptualization of privacy in the digital era. Along those lines we first need to acknowledge that people increasingly sacrifice voluntarily some of their privacy to enjoy the benefits of technology. Second, the ready availability of a huge volume of personal information creates attention scarcity, such that the chances a person's privacy will be intruded are diminished. Most importantly, though, once the law accepts the inevitability of the collection of personal information, it will be best in the position to focus attention on ensuring that the collected information is appropriately used, instead of wasting resources on trying to hinder in vain its collection. This more realistic approach calls for alternative means of regulation, like self-regulation or emphasis on informed consent, and facilitates the flow of information by reducing the transactional cost of its sharing and dissemination.

I. INTRODUCTION

"Congratulations on your colonoscopy" shouted Alan Shore in the courtroom making Judge Nora Lang blush with embarrassment. Too much information? "This is just information I was able to obtain from websites which employ the business standard for Internet security" he went on to explain (Boston Legal, Season 2, Episode 13).

Have we really reached a point where such sensitive information is so easily accessible to a fluffy

DOI: 10.4018/978-1-60960-083-9.ch003

non-tech savvy lawyer? And if what confuses you is the imaginary setting I use to ask the question consider the real case of Justice Antonin Scalia of the United States Supreme Court, for whom -as of last spring- we know his home number, the movies he likes, his food preferences, his wife's personal e-mail address, and what his grandchildren look like. You can thank Professor Joel Reidenberg and his students at Fordham Center on Law and Information Policy for that (Cohen, 2009).

What these two cases, and countless others both in the real and the TV world, have in common is the underlying facilitating effect of technology. And most often in egregiously intrusive cases like the above our almost instinctive reaction is to look for ways to limit the pervasiveness of technology. We fail, however, to see that in a historical perspective the trajectory of technological developments invariably attacks the notion of privacy, and –I argue- will continue to do so. There is indeed no reason to believe that, since technology has progressively enabled us to access more and more information, some of which private, we can somehow prevent this pattern from continuing into the future.

This is a theory of technological determinism in the realm of privacy. My argument is that digital technology, as best exemplified by digital networks, is bound to clash with privacy, and that the more it advances the fainter the privacy will become. Part II will explain the deterministic interaction between technology and privacy. In so doing I will show how privacy has materially shrunk due to the pressures exerted by new technologies and I will try to prove that this tendency will continue into the future. In the third part my aim is twofold: first, establish that privacy is overrated and that people in fact often give it up (deliberately or not) when this is accompanied by benefits, and second, offer general principles of how the law and people should approach the new concept of minimized privacy.

II. THE DETERMINISTIC INTERACTION OF TECHNOLOGY AND PRIVACY

1. Introducing Technological Determinism

Technological determinism is a charming, yet highly contested theory that never really found the acceptance it deserved in the humanities. This is partly attributable to the lack of a generally agreed on definition; as a result supporters of technological determinism are dispersed and uncoordinated (Bimber, 1994, p. 80). For some it states nothing more than the obvious, namely that technology has a role in fixing the form or the configuration of something (Winner, 1978, p. 75). As Heilbroner puts it "that machines make history in some sense … is of course obvious" (1967, p. 335). So obvious indeed that he rushes into the next sentence to explain that it is equally clear "that they do not make *all* of history" (Heilbroner, 1967, emphasis added).

On the other end of the spectrum technology is given the role of society's base, the fundamental and most important condition that effects a change (White, 1949, p. 366). In that sense social interactions, market forces and regulatory choices are mainly directed by technology. Needless to say that this radical view of the fate of human existence is both hard to accept and probably easily refuted. What does for example the invention of antibiotics (voted as the most important invention of the 20th century, see Lemelson-MIT Survey, 1999) say by itself for the evolution of the human kind? The extension of longevity is a direct corollary of antibiotics, but this is merely a fact. The meaning and ramifications of an extended lifetime for the human kind do not inadvertently flow from the invention of antibiotics itself. Most importantly, though, the problem with the extreme form of technological determinism is the difficulty we face when trying to reconcile the edifice of human logic with the no-choice state extreme

technological determinism leaves us with. As Lafollette and Stine explain "[a] new technology presents society with new capabilities, accompanied by new moral *dilemmas*; …technological developments represent neither *automatically* reliable nor necessarily positive outcomes" (1991, p. 1, emphasis added). This line of thought seems reasonable and is further confirmed by everyday practice as to when, where and how we *choose* to use technology.

In-between the two extremes (technology as the defining factor of change and technology as a mere tangent of change) and in a multitude of combinations falls the so called soft determinism; that is, variations of the combined effect of technology on one hand and human choices and actions on the other (Smith & Marx, 1994, p. xiii). The scope of soft determinism is unfortunately so broad that it loses all normative value. Encapsulated in the axiom "human beings do make their world, but they are also made by it," soft determinism is reduced to the self-evident (Winner, 1978, p. 88).

By now I have brought myself in a precarious position: I pledged to preach the deterministic effects of digital technology on privacy, yet at the same time I admit that technological determinism is either too extreme to be tenable or too obvious to be of value. I believe a compromise can be reached by mixing soft and hard determinism in a blend that reserves for technology the predominant role only in limited cases, one of which is the one at hand –privacy. Naturally, it is impossible to disregard the important contribution of political will, market choices and user habits in how technology ends up affecting our lives (Volti, 2006, pp. 271-283). However, my argument is that there are indeed technologies so disruptive that by their very nature they cause a certain change *regardless* of other factors. Some points of clarification are due here.

First, neither all technologies nor technology *per se* are determinative. This is the fundamental difference with hard determinism, which suggests that technology in general has a determinative effect. On the contrary, I use technological determinism here to refer to only *specific* technologies that are tied with *specific* results. One of these technologies is digital processing and one of these results is the elimination of privacy. One of course would reasonably ask what technologies are then deterministic. There is no easy answer to this question but in any case it is outside the scope of the analysis undertaken here. Though one could imagine a pattern behind deterministic technologies and use it to predict which nascent technologies will have deterministic effects (and maybe also what these effects will be), things get even more complicated considering that a technology can be deterministic in one context (say in Europe) but not in another (say in the USA) (Flichy, 2007, p. 24).

Second, since the specific technology is deterministic it leads to a result regardless of other factors. This is not to say that other factors are absent, but merely that the said technology is a *sufficient* condition to incur the change. This is the fundamental difference with soft determinism, which sees change as a *confluence* of a variety of factors, merely *one* of which is technology.

Lastly, and in relation to the preceding point, it needs to be stated that, while the end result is predetermined by the transformative technology itself, the details of how this result will be brought about as well as its precise configuration may be spelled out by the rest of the factors through complex interactions among them. The margin left for the rest of the factors to fill in the intermediate details, however, does not change the determinative nature of a given technology.

To synthesize what I have presented so far consider the example of the microwave technology as applied in American telecommunications. There is a wide consensus that the introduction of the microwave technology, which allowed the exchange of information (video, voice etc) via the electromagnetic spectrum over the air, is the primary cause of the end of AT&T's long-distance calls natural monopoly (Nuechterlein & Weiser, 2005, pp. 14-15). The reason is that microwaves

significantly dropped the cost of laying a long-distance network (which would normally be deployed on landlines) thereby allowing for the entry of competitors in the field. The primary rationale behind natural monopolies is to avoid duplication of the very costly required infrastructure, which would be wasteful due to the economies of scale and scope utilities like telecommunications exhibit (Geddes, 2000, p. 1183). Once the technological potentials for viable competition became available the quintessential reason of having a monopoly regime collapsed and the marked transitioned into competitive mode, despite the vehement opposition by established interests (most notably AT&T, see FCC, 1959, §148). The details of how the new scheme would work were laid down by the ensuing regulatory and market decisions, but the general direction of liberalization was already in place owing to the dynamics that the new technology had created. While there was no objective or extrinsic reason why the microwave technology would not be treated the same as the wireline system, the new dynamics were impossible to ignore and it is highly unlikely that the regulation of microwaves would be so uninspired as to merely replicate a network system analogous to the wireline system. The new technology innately carried a well-defined change in its shell.

Now that we are past the fundamentals of technological determinism I will use the remaining space of this part to explain why the advancement of digital technology is ineluctably bound to have a destructive impact on privacy.

2. Technological Progress and the Inescapable Loss of Privacy

As mentioned in the previous part it is hard –if not impossible- to predict which technologies are deterministic. This is mainly because knowing the future end result with which the technology is tied is a *sine qua non* to concluding on the deterministic nature of a given technology. And as we all know seeing into the future is a risky business. But for the purposes of telling whether digital technology has a predetermined destructive effect on privacy, it is enough to provide adequate evidence that, if put into a continuum, forms a consistent line toward less privacy. This argument presupposes that past dynamics will continue into the future, a theory that is safe to follow in lack of self-contradictory evidence. Unless of course one is inclined to adopt Hume's objections to causation, but I am willing to run that risk.

We also need to come up with a working definition of privacy. Technological determinism necessitates a broad view of privacy for it is a theory oblivious to the definitional differences among national legislations and, besides, privacy is inherently "a broad, abstract and ambiguous concept" (Griswold v. Connecticut (1965), Justice Black's dissent, p. 509). Under that broad understanding privacy would include all activity and all information that the subject has a reasonable expectation to keep to himself, the expectation to be free from unwarranted governmental or private intrusion, the option not to become the object of attention, the right to remain anonymous, and the ability to block physical access to himself (Gavison, 1980, pp. 428-436; Frombolz, 2000, pp. 463-464). An attack to privacy therefore should be construed as a violation, deprivation or limitation of any of the above rights and options. Additionally, since privacy is largely based upon a person's expectations and is experienced as an expression of individual autonomy (Henkin, 1974, p. 1425) any *threat* of loss of privacy or any precarious situation that endangers privacy should also count as an attack to privacy.

So the question now to ask is why digital technology results in the multiplication of threats or actual violation of privacy rights. The answer is to be found in the differences that digital technology bears in comparison to the previous real and analog world. In the analog era collecting personal information meant *physical* access. Access either to files where private information was retained or access to the premises where the person was.

Digital technology changed the playfield in that it allowed cheap, instant and accurate transfer of information without regard to the size or type of the information quantum or the distance between the place where the information was collected and the place where it was transmitted or processed. Since in the digital world a bit is a bit, meaning that all information is treated the same by the machines that collect, read, process, store and transmit it, the proliferation of digital technology in general entailed a concomitant spawning of devices that could be used or were exclusively designed for the collection of (personal) information. Examples range from voice recorders to surveillance cameras, to radio-frequency identification tags (*see*Froomkin, 2000, p. 1468-1501). But the exemplary application of technological determinism is to be found in digital networks and this will be my focus here.

As a first step consider the email. It became popular alongside the commercialization of the Internet and it wouldn't be a hyperbole to say that today almost all Internet users have an email address. What is interesting is that almost half of the total number of Internet users (also) has a web-based mail address, like@yahoo.com.In fact, the three major webmail services, Yahoo Mail, Hotmail and Gmail cumulatively count 700 million users, which translates to about 45% of the total Internet population. All the messages sent and received through a webmail service circulate freely in the Internet's wires and reside not on the local user's computer but on the remote servers of the provider company. This means that interception of and access to the emails can be obtained from anyone and anywhere in the world with standard PC equipment at a cost of less than $400. To contrast that with the real world the analogy of accessing one's mail would involve stalking and attacking the postman or breaking into the person's home. I am not trying to make an argument of legality –both actions are clearly illegal- but merely show how much easier it is to access someone's emails when they are stored online than to access his mail locked in a drawer. Understandably, one needs special expertise to hack into someone's account, but so does a burglar. On top of that, and most importantly, the potential pool of burglars is strictly localized[1] whereas the potential pool of hackers is 1,6 billion Internet users, the decisive element here being that the intruder needs to have *physical* access to the content he wishes to get hold of.

Imagine now that, instead of only your emails being stored online, you also start uploading the entire content of your hard drive. While on first thought this sounds like something that no rational user would do, in fact it is called online backup (or remote backup service) and it is currently estimated to support a $715 million market and growing (Chandler, 2008). At the same time a recent trend dating back to the early 00s allows users to upload selected personal information about themselves, usually accompanied by pictures, and share them with their friends. In only a matter of half a decade the most popular of these services, Facebook, grew to include more than 400 million active users, with more than 3 billion photos uploaded to the site each month (Facebook, 2010).

But all these technologies and services aside, the example that probably best illustrates how vulnerable privacy has become is cloud computing. Since cloud computing is more of a marketing term only a loose definition can be given here: a scalable network of servers on which users store data and use its processing power to run applications and services whose output is transmitted to the user's computer (Chappell, 2008). Arbitrary as it may sound, there is no commentator in the literature that has not emphasized the perils cloud computing poses for privacy (see for example Smith, 2010). And for a good reason indeed because cloud computing allows the user to emulate his personal computer online, including the applications he used to run locally and the data he used to store locally. So take GoogleDocs for instance. To use it the user connects to the application online, types the document online and saves it online,

precisely as he would do with Microsoft Word on his own personal computer. The difference is that the software, the storage and the processing power all reside in "the cloud," somewhere, that is, in Google's data farms. To put it in a nutshell cloud computing is about completely migrating online.

Now if we follow the pattern behind the technological evolution of digital networks, it must be obvious even to the eyes of the layman that the more technology progresses the more information escapes our *immediate physical control*. The element of physicality makes a world of difference, especially when it comes to illegal acts. No better case illuminates this point than digital piracy; although the net financial harm is the same in both cases, almost everyone has probably succumbed to digital piracy at least once, while very few would break the law by stealing a real CD from a music store (Stylianou, 2009, pp. 394-395). Similarly, while it would require a true criminal mind to break into someone's house and steal information, sending out a phishing email to commit identity theft suddenly sounds more innocuous. This reduced disapprobation in conjunction with the relative easiness technological intrusion comes with, is enough to render privacy readily susceptible to destructive attacks.

I do acknowledge, however, that some information put online can be encrypted and password protected and hence well guarded from unauthorized access. Yet we often fail to see how much personal information we give away voluntarily and for free. I will come back to this point later; suffice it to say here that we should not understand the clash between technology and privacy as a war between what individuals want and what technology imposes, but rather as a conflict of interests between privacy rights and technological benefits and capabilities. In this vein privacy simply ends up limping behind other priorities, most notably technological progress and the craving for new products and services. This is precisely the quintessence of technological determinism, namely that *in the name of new technological vistas which maximize access to information privacy folds*. Whether our life becomes more transparent voluntarily (e.g. Facebook) or contrary to our will (e.g. government surveillance) is immaterial. In either case the bottom line is that we keep inventing and adopting technologies that along with all their benefits compromise our privacy.[2]

Once we fully come to terms with this inevitability we can embark on a reconceptualization of what privacy means in the digital world and how to reconcile the unstoppably galloping technological progress with the projections of ourselves in the future. This is the focus of the next section.

III. A NEW MIND FRAME FOR PRIVACY IN THE DIGITAL WORLD

1. Setting the Hierarchy: The Real Value of Privacy

Privacy is overrated, but we have yet to realize it. By that I don't mean that privacy has ceased to be important, but rather that in relative values it is ultimately not as big a concern as is commonly perceived. This misperception stems from the fact that when asked, people always appear worried about the transparency of their personal lives. For example a recent cloud computing survey by Microsoft found that "more than 90 percent of [the] people are concerned about the security, access and privacy of their own data in the cloud" (Microsoft, 2009). But at the same time the same survey showed that 90 percent of Americans are using some form of cloud computing (Microsoft, 2009). Combine the two and the conclusion to be drawn is that people's choices suggest that the potentials of a new technology outweigh the privacy costs. Similarly while many people have expressed their unease with privacy protection in social networking sites, we see an explosive growth in the information they post online and the activities –some of them very intimate- they

undertake in the frames of digital social networks (Ito et al., 2009, pp. 13-34).

This trend toward more sharing of personal information is justified by the offsetting effects of technology. People acknowledge the overwhelming benefits of technology and yield to them at the expense of privacy. The benefits can be varied. A study for example showed that Facebook users are inclined to divulge increasingly more personal information based on the belief that there will be a concomitant increase in their popularity (Christofides, 2009, p. 343).

In a different setting, users of the Gmail service were enticed to sacrifice some of their privacy in exchange for more inbox space. When Gmail was first introduced in 2004 it was severely criticized for its data retention policy and its ad-supported scheme, whereby users' emails were scanned for keywords so that personalized advertisements could be fed to them (Miller, 2005, passim). These concerns notwithstanding, when it became known that Gmail's capacity would be 1GB compared to the meager 4-10MBs Yahoo! and Microsoft (Hotmail) offered, users started flocking to Gmail. Today, Gmail remains the most pervasive email platform but its users pool nevertheless counts 150 million users, ranking third behind Yahoo! and Hotmail.*

A change in moral and social standards can also result in a downgrading of privacy. The ongoing study about the future of the Internet conducted by the Pew Internet and American Life Project and Elon University is very helpful at this point. Every two years participants are asked to discuss possible scenarios for 2020 with regard to Internet issues. In the 2006 survey 46 percent of the respondents agreed that the benefits of greater transparency would outweigh the privacy costs and 49 percent disagreed (Anderson & Rainie, 2006, pp. i-ii). Interestingly, in the 2008 survey the percentage of the people that disagreed with the statement that "in 2020 people are even more open to sharing personal information … [and] are generally comfortable exchanging the benefits of anonymity for the benefits they perceive in data being shared…" dropped to 44 percent (Anderson & Rainie, 2008, p. i).

It seems that in final analysis people are not completely hostile to the overriding effects of technology despite their *prima facie* objections. Naturally, if we were given the choice to be able to enjoy all the benefits of digital social networking without compromising our privacy at all, Facebook would be the ideal digital world. However, given the present state of affairs, I want to take the previous arguments one step further and suggest that some *involuntary* leak of private information is not necessarily as evil as we seem to think.

Take behavioral advertising for example. Behavioral advertising involves the automated collection of web browsing data from advertisers who then use it to serve targeted advertisements to consumers. As expected, the large majority of users reject behavioral advertising for fear of privacy intrusion (Turow et al., 2009, p. 3). But this finding has to be read in a context. The same survey also concluded that users would still oppose behavioral advertising even if their anonymity was guaranteed (Turow et al., p. 4). This implies that users are hostile toward behavioral advertising in general, regardless of whether it is intrusive or not. This is possibly because advertisements of any kind are usually a nuisance to them, so why not avoid them altogether if given the option?

Most importantly, though, we need to ask a more fundamental question and I will state it here in general terms: why is it in the end so important for us to protect our private data from being collected and/or used? The importance of this question lies in that we can demystify privacy if we acknowledge that sharing private information is less risky than what we usually think. As Jeffrey Reiman has put it "a threat to privacy is only worrisome insofar as privacy is valuable or protects other things that are valuable. No doubt privacy is valuable to people who have mischief to hide, but that is not enough to make it generally worth protecting" (Reiman, 1996, p. 29). Reiman

has nicely summarized the three pillars of the philosophical core of privacy, which can help us identify the reasons why we abominate the erosion of privacy: a) the *extrinsic loss of freedom*, also noted by other scholars as emanating from the right to *autonomy*, that is being able to choose for one's self what information becomes available (Westin, 1966, p. 1022), b) the *intrinsic loss of freedom*, that is the emotional state of knowing that one is free to make choices, c) the *symbolic function of privacy*, that is the institutional structure of privacy in society, and lastly d) in what he calls *the risk of psycho-political metamorphosis* –namely the impoverishment of inner life due to total visibility (Reiman, 1996, pp. 35-44).

I do not plan to take issue with any of the above justifications for privacy, which in any case I find at least to a certain extent valid. I do want, however, to qualify these common privacy concerns in a way that better reflects how technology threatens privacy. My position is that technology has made it indeed so easy to collect personal data that in many cases they have lost their individual value, and instead function merely as statistical or ancillary data. I am not claiming that the collected information does not amount to adequate data to synthesize a person's profile –quite the contrary (Picker, 2009, pp. 24-35), but rather that the true identity of a particular person is in principle indifferent to the aggregator of the information and hence no concern is warranted. In the case of behavioral advertising, for instance, a user's personal browsing history could potentially reveal a lot about his personality and life, but it is in fact seen as nothing more than input to the advertiser's algorithm that will calculate which advertisement is more relevant to serve (*cf.* O'Reilly, 2004 for Gmail's advertisement system). Another example is Google Street View, which provides 360° horizontal panoramic views from a row of positions along many streets in the world. This service necessarily pictures real people without their consent and in some cases they are caught in embarrassing situations like entering a sex-shop or being arrested (BBC, 2009). While I could concede that this constitutes an ad hoc invasion of privacy, it is important to note that the technology itself is not directly threatening to the individual, because, despite its technical *capability* of surveillance, the *probability* that it will be used for such purposes makes it practically innocuous. When millions of people have been randomly photographed in the street, a particular person's shot does not amount to invasion of privacy in essence, because there is nothing unique, specific or interesting about that particular person being photographed instead of someone else.

The risk about the further use and misuse of the collected information is a different issue, which I discuss in passing right below. For now and to conclude, my argument in this part could be summarized in these two strands: that privacy is likely overestimated, often because we fail to put the loss of privacy in perspective thereby exaggerating the potential –but rarely realizable- dangers, and that even when the dangers are real, people are often willing to compromise their privacy for the benefits a given technology has to offer. Seen in this light it is no wonder that the trajectory mandated by technological developments overlooks, bypasses or straightforwardly eliminates privacy policies.

2. Securing Privacy in a Technologically Pervasive Environment

In this last part my endeavor is to reconcile the increasingly intrusive technology with the privacy interests as traditionally understood. Acknowledging the deterministic effects of technology is no excuse to sit idle and surrender to the march of intrusive technologies under the pretext that this is destined to happen. I repudiate this absolutist view, and in fact, I do not think that we will ever consent to passively waive the triptych of privacy: protecting privacy of individuals against intrusive governments, protecting personal or private information, and protecting places deemed

personal or private (Nissenbaum, 2004, pp. 125-131). However my major disagreement lies in the means with which we will secure this triptych. I favor a shift in emphasis from regulation of *collection* of data to regulation of *use* of data. This shift is predicated precisely upon the fact that technology is making it increasingly easy to collect data (often legally) and therefore I'm afraid that regulation in the direction of controlling the collection of information will lead to a waste of resources that could be allocated elsewhere. In this new framework we reserve an important role for the law, but it is also social and technological norms that will significantly shape the new privacy protection context. In the words of Google's chief economist, Hal Varian, "[p]rivacy is a thing of the past. Technologically it is obsolete. However, there will be social norms and legal barriers that will dampen out the worst excesses" (quoted in Anderson & Rainie, 2006, p. v).

These social norms in the real world are easy to discern. In most countries people don't keep their window curtains closed, even though they know that they can be seen through the window. However, social norms mandate that it is not polite to stare through an apartment's window. Also, people usually think that there is no reason for someone to stare through their windows, and therefore the need to take precautionary measures is mitigated. In fact, these statements hold even more truth in the urban environment where people's relationships are less intimate and the opportunities to peek through a window are so abundant that they lose value.

The analogy to the contemporary digital environment is not hard to see. As the digital population grows bigger and more and more activities are added to our digital lives, our digital footprint becomes bigger but at the same time diluted. It is decades now that Herbert Simon, the pioneering American political scientist, pointed out that "a wealth of information creates a poverty of attention" (Simon, 1971, p. 40). Indeed, from the standpoint of the aggregator of information the vast volume of available information alone makes zeroing in onto one individual highly unlikely and practically useless. To go back to the Scalia experiment, what shields us from exposure is the fact that we are not as important -and perhaps provocative- as Justice Scalia is. When it comes to the average person privacy is ensured by attention scarcity, not by impediments in the collection of information. As technology advances our lives will increasingly be transformable to collectible data, so abundant in fact that aggregators will probably find it uneconomical to collect all of them (Steeves, 2008, p. 337). A good example of what was once unimaginable but today can constitute collectible information is the thermal images of one's presence in his house using an infrared camera. Regardless of whether this information is legal to obtain without a warrant, the key point is that in a real case such data was enough to alarm the police that a person may be cultivating marijuana (Kyllo v. United States, 2001; *see contra* R. v. Tessling, 2004 (Canada's Supreme Court)). This profuseness of information coupled with the law's notorious lag (or even complicity, *see*Rubenfeld, 2008) in deciding upon what constitutes protectable personal information –reasonably so as technology and human ingenuity is always a step ahead– is good grounds to argue that focusing on controlling the collection of information may no longer be an efficient policy, for the collection *will* take place one way or another (Brin, 1998, pp. 8-9).

Attention scarcity as described above ensures that information is harder to collect, and hence it serves as a means of securing privacy at the stage *before* information comes into custody. As we can see it is not a legal measure, but rather an endogenous quality of the digital networks architecture, or in other words an embedded safety valve to ameliorate the danger of privacy intrusion. On top of technology's inherent limitations, people and the market can also adopt measures to limit exposure. For example once people accept that their private information is easy to collect they

may want to consider the alternative of providing false or incomplete information (*cf*. Palfrey, 2008, Appendix C, p. 39; Burkell et al., 2007, p. 2; Ben-Ze'ev, 2003). The market can contribute its own share to this effort by helping consumers reach decisions regarding how much personal information they share or by making sure that consumers give their informed consent to the use of their personal information (Borenstein, 2008, pp. 24-25).

This approach of privacy admittedly leaves many theoretical issues unresolved. It completely marginalizes autonomy as the foundation of privacy (Cohen, 2000, pp. 1424-1428), and it is disrespectful to contextual integrity by treating all information the same regardless of the context in which it was collected and the context that it will eventually be used (Nissenbaum, 1998, pp. 581-586). This criticism is valid but it misses the point. Taking for granted that technology steadily facilitates the collection of information, the critique against a legal regime that does not maximize precautionary measures to combat the collection of information (and one that hence takes into account autonomy and contextual integrity) is misplaced. While of course the collection of information cannot be left unregulated, under the theory of technological determinism the law's primary response should focus on the stages *after* the information has been collected. The post-collection stage includes the use, processing and further transmission of the collected information. To take the case of behavioral advertising, a law influenced by technological determinism would loosen the restrictions placed on a website that collects anonymous information from the web history of the user, but would impose strict rules on what the company could do with the collected information, like for example that the company cannot use the information for purposes other than serving targeted advertisements.

There are two gains in this approach: first, it facilitates the flow of information and diminishes the transactional costs. Economic analysis of law would suggest that, when it is not imperative to keep information private –as in the case of anonymous web history data- removing free flow restrictions serves the public interest, as it allows the maximization of the information's value (Posner, 1978, pp. 394-397, 401-404). Second, for legislation to be effective it needs to stay in touch with the reality it purports to regulate. In a world where information *will* be collected, the law should consider focusing on more realistic measures without naively negating the power of technology and the determination of the market and the people to get what they want in the end. Again, this is not to suggest that regulation of the collection of information should cease to exist, but rather that the post-collection treatment of information is equally, if not more, important. In this vein, EU's new privacy rules that require the user's consent for every storing of information, or gaining of access to information in the user's terminal equipment, are in complete dissonance with the Internet's reality (*see* art. 5(3), Directive 2009/136/EC). Requiring the user to consent to the storing of every cookie on his computer is burdensome not only for the website operators but for the user himself. The pace of transactions on the Internet, the automated nature of the process of communication and the transactional customs on the Internet render EU's new measure utterly unrealistic and counter-productive. Instead, the EU should opt to facilitate the communication between web-services and users by allowing the installation of cookies, while at the same time commit to the protection of consumer privacy by prohibiting –for instance- surreptitious secondary uses of the cookies, sharing of collected information with other entities, long-term storage of cookies and any other measures that would ensure the limited and targeted utility of freely-flowing cookies.

Another flexible approach along the lines of more lenient regulation on the collection of information would be to promote self-regulation (Swire, 1997). For example in a laudable initiative

led by the American Association of Advertising Agencies the advertisements industry asks that "[t]hird Parties and Service Providers … give clear, meaningful, and prominent notice on their own Web sites that describes their Online Behavioral Advertising data collection and use practices" (AAAA et al., 2009, II.A.1). Self-regulation does not necessarily imply that the rule of law will be marginalized, but rather that the new privacy protection scheme will be a joint effort between those who possess the technological potentials and the state (Sinclair, 1997). In this scheme the final format of the regulation will fall somewhere between the two extremes of minimal protection pushed by the market and maximum protection pushed by the state.

From the preceding discussion it seems reasonable to infer that the thrust behind technological progress is so powerful that it is almost impossible for traditional legislation to catch up. While designing flexible rules may be of help, it also appears that technology has already advanced to a degree that it is able to bypass or manipulate legislation. As a result, the cat-and-mouse chase game between the law and technology will probably always tip in favor of technology. It may thus be a wise choice for the law to stop underestimating the dynamics of technology, and instead adapt to embrace it.

IV. CONCLUSION

This essay does not mean to suggest that the law is impotent. The herein presented theory of technological determinism simply highlights that technology may under certain circumstances develop its own independent path, which the law should not disregard, but rather adapt to it. In the case at hand, namely the intersection of digital technology and privacy, the first step is to reassess what privacy means in the digital world. It goes without saying that in interacting with technology people would prefer to keep most of their private information undisclosed, but this is not the right benchmark to use. Rather we need to look at how much privacy people are ready to sacrifice to enjoy the benefits of technology. What technological determinism teaches us so far is that people will always react negatively to more intrusive technology, but in the end they will probably succumb. Once we have established the true value of privacy, and given the dynamics of technology, the law should focus on producing legislation that facilitates the exchange of information on the one hand, but prevents misuse of that information on the other. This, in other words, translates into placing more emphasis on regulating what entities can do with the collected information, and into a gradual relaxation of regulation that hinders the collection of personal data. That said, this paper acknowledges that both types of regulation are necessary to provide a full framework of privacy protection.

ACKNOWLEDGMENT

I wish to thank Ms. Melina Kapeliou for her unconventional help in the completion of this essay.

REFERENCES

American Association of Advertising Agencies, Association of National Advertisers, Council of Better Business Bureaus, Direct Marketing Association, and Interactive Advertising Bureau. (2009). *Self-regulatory principles for online behavioral advertising*. Retrieved from http://www.iab.net/media/file/ven-principles-07-01-09.pdf

Anderson, J., & Rainie, L. (2006). *The future of the Internet II*. New York: Pew Internet. Retrieved from http://www.elon.edu/e-web/predictions/2006survey.pdf

Anderson, J., & Rainie, L. (2008). *The future of the Internet III*. New York: Pew Internet. Retrieved from http://www.elon.edu/docs/e-web/predictions/2008_survey.pdf

BBC. (March 20, 2009). *Google pulls some street images*. Retrieved from http://news.bbc.co.uk/2/hi/7954596.stm

Ben-Ze'ev, A. (2003). Privacy, emotional closeness, and openness in cyberspace. *Computers in Human Behavior*, *19*, 451–467. doi:10.1016/S0747-5632(02)00078-X

Bimber, B. (1994). The three faces of technological determinism. In Smith, M. R., & Marx, L. (Eds.), *Does technology drive history? The dilemma of technological determinism*. Cambridge, MA: MIT Press.

Borenstein, J. (2008). Privacy: A non-existent entity. *IEEE Technology and Society Magazine*, *27*(4), 20–26. doi:10.1109/MTS.2008.930565

Brin, D. (1998). *The transparent society: Will technology force us to choose between privacy and freedom*. New York: Perseus Books.

Burkell, J., Steeves, V., & Micheti, A. (2007). *Broken doors: Strategies for drafting privacy policies kids can understand*. Ottawa, Canada: On the Identity Trail. Retrieved from http://www.idtrail.org/files/broken_doors_final_report.pdf

Chandler, D. (2008). *Worldwide online backup services 2007-2011 forecast: A new market emerges*. Framingham, MA: IDC.

Chappell, D. (2008). *A short introduction to cloud platforms: An enterprise-oriented view*. Retrieved from http://www.davidchappell.com/CloudPlatforms--Chappell.pdf

Christofides, E., Muise, A., & Desmarais, S. (2009). Information disclosure and control on Facebook: Are they two sides of the same coin or two different processes? *Cyberpsychology & Behavior*, *12*, 341–345. doi:10.1089/cpb.2008.0226

Cohen, J. (2000). Examined lives: Informational privacy and the subject as object. *Stanford Law Review*, *52*, 1373–1437. doi:10.2307/1229517

Cohen, N. (2009, May 17). Law students teach Scalia about privacy and the web. *The New York Times*. Retrieved from http://www.nytimes.com/2009/05/18/technology/internet/18link.html

Directive 2009/136/EC of the European Parliament and of the Council. *Official Journal L337/11*.

Estelle T. Griswold & C. Lee Buxton v. Connecticut (1965), 381 U.S. 479.

Facebook. (2010). Press office statistics. Retrieved from http://www.facebook.com/press/info.php?statistics

FCC (1959), Allocation of frequencies in the bands above 890 Mcs, 27 FCC 359.

Flichy, P. (2007). *Understanding technological innovation: A socio-technical approach*. Northampton, MA: Edward Elgar Publishing.

Frombolz, J. (2000). The European Union data privacy directive. *Berkeley Technology Law Journal*, *15*, 461–484.

Froomkin, M. (2000). The death of privacy? *Stanford Law Review*, *52*, 1461–1543. doi:10.2307/1229519

Gavison, R. (1980). Privacy and the limits of law. *The Yale Law Journal*, *89*, 421–471. doi:10.2307/795891

Geddes, R. (2000). Public utilities. In Bouckaert, B., & De Geest, G. (Eds.), *Encyclopedia of law and economics*. Northampton, MA: Edward Elgar Publishing.

Griswold v. Connecticut, 381 U.S. 479 (1965).

Heilbroner, R. (1967). Do machines make history? *Technology and Culture*, *8*, 335–345. doi:10.2307/3101719

Henkin, L. (1974). Privacy and autonomy. *Columbia Law Review*, *74*, 1410–1433. doi:10.2307/1121541

Ito, M., Horst, H., Bittanti, M., Boyd, D., Herr-Stephenson, B., Lange, P. G., & Pascoe, C. J. … Tripp, L. (2009). *Living and learning with new media: Summary of findings from the digital youth project (The MacArthur Foundation reports on digital media and learning)*. Cambridge, MA: MIT Press.

Kyllo v. United States, 533 U.S. 27 (2001).

Lafollette, M., & Stine, J. (1991). Contemplating choice: Historical perspectives on innovation and application of technology. In Lafollette, M., & Kline, J. (Eds.), *Technology and choice: Reading from technology and culture*. Chicago: University of Chicago Press.

Lemelson-MIT Program. (1999). Lemelson-MIT survey finds high school students, their parents agree—and disagree—on the most important 20th century inventions [Press release]. Retrieved from http://web.mit.edu/invent/n-pressreleases/n-press-99index.html

Microsoft. (2009). Cloud computing flash poll – Fact sheet. Seattle, WA: Microsoft. Retrieved from www.microsoft.com/presspass/presskits/cloudpolicy/docs/PollFS.doc

Miller, J. I. (2005). Don't be evil: Gmail's relevant text advertisements violate Google's own motto and your E-Mail privacy rights. *Hofstra Law Review*, *33*, 1607–1641.

Nissenbaum, H. (1998). Protecting privacy in an information age: The problem of privacy in public. *Law and Philosophy*, *17*, 559–596.

Nissenbaum, H. (2004). Privacy as contextual integrity. *Washington Law Review (Seattle, Wash.)*, *79*, 119–158.

Nuechterlein, J., & Weiser, J. P. (2005). *Digital crossroads: American telecommunications policy in the Internet age*. Cambridge, MA: MIT Press.

O'Reilly, T. (2004). *The fuss about Gmail and privacy: Nine reasons why it's bogus*. Sebastopol, CA: O'Reilly. Retrieved from http://www.oreillynet.com/pub/wlg/4707

Palfrey, J. (2008). *Enhancing child safety and online technologies*. Cambridge, MA: The Berkman Center for Internet & Society, Harvard University. Retrieved from http://cyber.law.harvard.edu/pubrelease/isttf/

Picker, R. (2009). *Online advertising, identity and privacy (University of Chicago Law & Economics, Olin Working Paper No. 475)*. Retrieved from http://ssrn.com/abstract=1428065

Posner, R. (1978). The right of privacy. *Georgetown Law Review*, *12*, 393–422.

Reiman, J. (1996). Driving to the panopticon: A philosophical exploration of the risks to privacy posed by the highway technology of the future. *Santa Clara Computer and High-Technology Law Journal*, *11*, 27–44.

Rubenfeld, J. (2008). The end of privacy. *Stanford Law Review*, *61*, 101–161.

Simon, H. (1971). Designing organizations for an information-rich world. In Greenberger, M. (Ed.), *Computers, communications, and the public interest*. Baltimore, MD: Johns Hopkins Press.

Sinclair, D. (1997). Self-regulation versus command and control? Beyond false dichotomies. *Law & Policy*, *19*, 529–559. doi:10.1111/1467-9930.00037

Smith, B. (2010, January 20). Cloud computing for business and society. *The Huffington Post*. Retrieved from http://www.huffingtonpost.com/brad-smith/cloud-computing-for-busin_b_429466.html

Smith, M., & Marx, L. (Eds.). (1994). *Does technology drive history? The dilemma of technological determinism*. Mass: MIT Press.

Steeves, V. (2008). If the Supreme Court were on Facebook: Evaluating the reasonable expectation of privacy test from a social perspective. *Canadian Journal of Criminology and Criminal Justice*, *50*, 331–347. doi:10.3138/cjccj.50.3.331

Stylianou, K. (2009). ELSA copyright survey: What does the young generation believe about copyright? *Intellectual Property Quarterly, 2009*(3), 391-395.

Swire, P. (1997). Markets, self-regulation, and government enforcement in the protection of personal information. In Daley, W. M., & Irving, L. (Eds.), *Privacy and self-regulation in the information age*. Washington, DC: U.S. Department of Commerce.

Tessling, R. v. (2004). 3 S. *CR (East Lansing, Mich.)*, 432.

Turow, J., King, J., Hoofnagle, C. J., Bleakley, A., & Hennessy, M. (2009). *Americans reject tailored advertising and three activities that enable it*. Retrieved from http://ssrn.com/abstract=1478214

Volti, R. (2006). *Society and technological change*. New York: Worth Publishers.

Westin, A. (1966). Science, privacy, and freedom: Issues and proposals for the 1970's: The current impact of surveillance on privacy. *Columbia Law Review*, *66*, 1003–1050. doi:10.2307/1120997

White, L. (1949). *The science of culture*. New York: Farrar, Straus & Giroux.

Winner, L. (1978). *Autonomous technology: Technics-out-of-control as a theme in political thought*. Cambridge, MA: MIT Press.

ENDNOTES

[1] I assume that the cost of traveling to a foreign or far-away place and the processing cost of carrying out the crime at that place exceed the benefit that the burglar will get.

[2] This is meant to be a descriptive statement. I am not claiming that loss of privacy is necessarily a negative outlook, as I am not endorsing the opposite view either.

[*] The reasons it only ranks third are unrelated to technology. Yahoo and Microsoft had a significant lead-time advantage during which they managed to build a robust and extensive clientele. Also, Yahoo! and Hotmail took advantage of economies of scope and networking effects by bundling their email services with Instant Messaging capabilities.