Karl-Friedrich Lenz

Digital Rights Management (DRM) and Data Protection

I. Introduction

I have discussed a number of questions related to DRM on my blog.[1] In this paper, I want to focus on the relation to data protection.

This question needs to be discussed. I agree with *Bechtold*, who recently stated[2] that this relation is in need of clarification:

"While it is still unclear what role DRM should and will play in the intellectual property system, its relation to other areas of law is fuzzy as well. This applies particularly to privacy law."

I also agree with *Cohen*'s opinion:[3] "Quite apart from the questions of intellectual property policy that surround DRM technologies, therefore, the proper balance between DRM and user privacy is an important question on its own right."

And the European Consumers' Association BEUC[4] has requested[5] the Article 29 Working Party to issue an opinion on how to interpret the European data protection rules in the context of DRM in February 2003.

Stallman's famous essay about "The Right to Read"[6] shows clearly the dangers of ignoring privacy considerations when discussing DRM. He draws a bleak picture of a

---

[1] Search for "DRM" at k.lenz.name/LB.

[2] Bechtold, Stefan, The Present and Future of Digital Rights Management, Musings on Emergent Legal Problems, in: Eberhard Becker, Willms Buhse, Dirk Günnewig, Niels Rump (eds.), Digital Rights Management: Technological, Economical, Legal and Political Aspects, Springer, Berlin, 2003, 597, 617 (online at www.jura.uni-tuebingen.de/bechtold/pub/2003/Future_DRM.pdf).

[3] Cohen, Julie E., DRM and Privacy, www.law.berkeley.edu/institutes/bclt/drm/papers/cohen-drmandprivacy-btlj2003.html (2003). See also Cohen, Julie E., The Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace, www.law.georgetown.edu/faculty/jec/read_anonymously.pdf (1996).

[4] Bureau Européen des Unions de Consommateurs, Welcome to BEUC, www.beuc.org.

[5] BEUC, BEUC comments on the 95/46/EEC Directive on Data Protection, europa.eu.int/comm/internal_market/privacy/docs/lawreport/paper/beuc_en.pdf (February 2003).

[6] Stallman, Richard, The Right to Read, www.gnu.org/philosophy/right-to-read.html (1996, with update 2002).

society where all reading is reported to the "Software Protection Authority". This kind of extreme surveillance would, of course, violate human rights and European data protection standards. It probably could not be introduced right now. However, steps into the direction of total surveillance of reading are quite possible. These dangers need to be recognized early on, so they can meet with the appropriate level of resistance by anyone interested in preserving human rights.

Of the many possible aspects of the relation between DRM and data protection, I will discuss three questions in this paper: Anonymous use of the Internet, data protection aspects of trusted computing, and data protection concerns against the proposal of a Directive on the enforcement of intellectual property rights.

I am going to state my point of view on these questions and then discuss European law regarding them.

II. Anonymous Internet use

1. My point of view

Why is the question of anonymous Internet use important for the discussion of DRM?

I agree with *Felten*[7] that the first thing you need to talk about when addressing DRM is your threat model.

And that requires understanding the point made in the May 2003 paper of *Schechter*, *Greenstadt*, and *Smith*.[8] That point is: There are costs of extracting content from its protected form and costs of distributing that content. And they reach the surprising conclusion that deployment of "trusted computing" might actually help to reduce distribution costs by protecting P2P networks against attacks by the copyright holders. That would mean that "trusted computing", which might be expected to help copyright holders protect their content, would work in the opposite direction.

If you try to build an informational infrastructure where it is impossible to extract content from its protected form, you are very likely to fail. *Schneier* has pointed out

---

[7] Felten, Ed, DRM, and the First Rule of Security Analysis, www.freedom-to-tinker.com/archives/000317.html (March 2003); The Broadcast Flag, and Threat Model Confusion (November 2003), www.freedom-to-tinker.com/archives/000469.html.

[8] Schechter, Stuart E., Greenstadt, Rachel E., Smith, Michael D, Trusted Computing, Peer-to-Peer Distribution and the Economics of Pirated Entertainment, www.eecs.harvard.edu/~stuart/papers/eis03.pdf.

years ago that this is basically hopeless.[9] And *Felten* has explained[10] this as well, comparing the DRM situation to an armoured truck carrying money from a WalMart store to the bank. The moment the truck doors open at the bank, the money is not protected any more by that truck. But you need to deliver at some time to the bank. And in the DRM scenario, the "bank" is your opponent who is trying to break your DRM system. At the very least, a dedicated pirate can use a microphone and a camera to record whatever is delivered to the human ear and eye.[11]

If it is hopeless to keep content from being extracted, at least if your opponent is dedicating large resources and expertise to the extraction, all DRM technology dealing with that threat model is only a side show. The real battle will be over the distribution costs.

Without copyright, distribution costs would be near zero. The Internet makes the planet very small. Knowledge and culture could spread at the speed of light over the net. That is in strong contrast to earlier centuries. Three thousand years ago, the spread of knowledge and culture took much time. And the fact that this spread of knowledge was somewhat faster in Europe than in Africa might have contributed to the faster development of technology in Europe. That is *Diamond*'s claim.[12] He says that one of the reasons for the European superior position throughout most of recorded history lies in the fact that Eurasia spreads from West to East, while in contrast Africa and America spread from North to South. That in turn, according to *Diamond*, made it easier for knowledge to spread faster.

I am not sure if *Diamond's* explanation of the European technological advantage is correct or not.[13] However, one thing is clear. Today, all barriers to the spread of knowledge and culture that remain are artificial, based on the legal system. If copyright and patent law were abolished on a worldwide scale tomorrow, knowledge and culture could spread instantly over the whole planet. That is probably not likely to happen anytime soon. But I think it is important to understand that copyright and patent law

---

9 Schneier, Bruce, The Futility of Digital Copy Prevention, www.schneier.com/crypto-gram-0105.html#3 (May 2001); Software Copy Protection, www.schneier.com/crypto-gram-9811.html#copy (November 1998).
10 Felten, Ed, Why Unbreakable Codes Don't Make Unbreakable DRM, www.freedom-to-tinker.com/archives/000214.html.
11 Schechter/Greenstadt/Smith, supra note 8, 5-6.
12 Diamond, Jared, Guns, Germs and Steel, 1997.
13 For more detail about this see Lenz, Karl-Friedrich, Grenzen des Patentwesens (2002), 13-15.

are the only remaining obstacles to instant spread of knowledge and culture.[14]

With copyright, distribution costs may be calculated as the risk of getting caught and sued by the copyright owner, multiplied with the average cost that causes. *Solum* does exactly that kind of multiplication when discussing the recent RIAA lawsuits, writing:[15] "Even thousands of lawsuits is a drop in the bucket when tens of millions use file sharing services. Assume that being sued and settling creates an average cost of $10,000, and that the average user of a file sharing program has a 1 in 20,000 chance of being sued. (2,000 suits/20,000,000 users). That's 50 cents of expected cost. I think my calculations actually exaggerate the costs, but they come within an order of magnitude". [16].

Obviously, the risk of being caught will be strongly influenced by the amount of data protection on the Internet.

If the copyright owner can easily track down individual users, the expected cost will be much higher than 50 cents.

If on the other hand the file traders can hide behind a strong and reliable wall of anonymity, distribution costs will stay at the extremely low level they would be without copyright, since copyright can't be enforced if you can't name a defendant for your lawsuit.

If everybody can use a P2P network, so can the copyright holder. That gives copyright holders IP numbers of people infringing their copyrights by posting their works.

Then they need to match that IP number to a person, get a name and address matching the IP number.

For that, they usually need the cooperation of the Internet service provider who owns that IP number. That provider might look up which customer used the IP number at the time and give that information to the copyright holder.

To do that, the service provider must be able and willing to do so.

---

[14] See also Gilmore, John, What's Wrong With Copy Protection, www.toad.com/gnu/whatswrong.html (2001).
[15] Solum, Lawrence, RIAA Lawsuit Offensive Begins, lsolum.blogspot.com/2003_09_01_lsolum_archive.html#106313634911633894.
[16] I have not corrected the obvious calculation error in *Solum's* text. Of course, dividing 20 million by 2000 gives a result of 10.000, not of 20.000. However, this doesn't matter very much. His point is clear enough anyway. And I certainly agree with it.

The service provider is not able to do so if he doesn't keep any log files in the first place. That leads to the question if service providers are required to keep log files. Or, quite on the contrary, they are required to erase all traces of an individual communication as soon as it ends. There is a heated debate about exactly that question. I have commented on that before,[17] but I want to take another look at this now.

So there is a conflict between data protection for Internet users and the interest of copyright holders in raising the distribution costs for illegal copies. How should that conflict be resolved? This is the first question I am going to discuss in this paper. And my position is:

Retention of traffic data is prohibited by Article 6 of the 2002 communications data protection directive.[18]

As well it should be.

Confidentiality of communications is a human right. It is guaranteed in Article 8 of the 1950 Convention for the Protection of Human Rights and Fundamental Freedoms.[19] The Working Party on the Protection of Individuals with Regard to the Processing of Personal Data has pointed this out already in 1999, with some references to the relevant case law of the European Court on Human Rights.[20] And it has pointed it out again[21] and again.[22]

Traffic data retention violates that human right. With the Internet, knowing the page

---

[17] Lenz, Karl-Friedrich, Kanshigata intahnetto hiteiron (Against Internet surveillance), Aoyama Hogaku Ronshu 42-4 (2001); Traffic Data, k.lenz.name/LB/archives/000209.html (March 2003).

[18] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), europa.eu.int/eur-lex/en/lif/reg/en_register_132060.html.

[19] Convention for the Protection of Human Rights and Fundamental Freedoms, conventions.coe.int/Treaty/EN/CadreListeTraites.htm.

[20] Working Party, Recommendation 3/99 on the preservation of traffic data by Internet Service Providers for law enforcement purposes, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/1999/wp25en.pdf, 4-5.

[21] Article 29 Data Protection Working Party, Opinion 4/2001, On the Council of Europe's Draft Convention on Cyber-crime, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2001/wp41en.pdf.

[22] Article 29 Data Protection Working Party, Opinion 5/2002 on the Statement of the European Data Protection Commissioners at the International Conference in Cardiff (9-12 September 2002) on mandatory systematic detention of traffic data, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_en.pdf.

someone has been using means knowing the content of his communication. Keeping traffic data records on all Internet users is the equivalent of recording all telephone conversations of all citizens. Not acceptable under any reasonable standard of human rights protection.

It won't do to have all citizens watched at all times.

Internet traffic data retention is not necessary for billing purposes. Therefore Internet traffic data must be deleted immediately.[23] With the telephone network, it makes a difference if a call is local or international. When using the Internet, the price is always the same. It makes no difference for billing if the pages you are using are located next door or if they are located on the other side of the planet.

Traffic data retention might be useful for prevention and investigation of crime.

But so would be watching everybody 24 hours a day over video cameras, implanting chips in all citizens' skulls to track all of their movements, or imposing an obligation to carry a handy and leave it switched on at all times (enabling the police to listen in on conversations).

All of which would be completely out of the question.

So the fact that some measure might be useful to reduce crime is not enough to justify its privacy cost. The question is one of proportion. Between the privacy cost on one side and the usefulness for crime prevention on the other side.

And the usefulness for crime prevention of watching all citizens at all times is rather limited in the first place. Of course every criminal worth paying any attention to will know that his Internet activity will be logged. So criminals will use countermeasures. Just as you can't expect a bank robber to use his own car with his own number plate to drive up to the bank, you can't expect a serious criminal to use the Internet under his own name from his own account.

Some criminals might be stupid enough to be caught by looking at log files. That possibility exists. But on the other hand, the law enforcement community is in no particular lack of information to analyze even now. It's the other way round. They have access to so much data that they are overwhelmed and can't make efficient use of that

---

[23] Article 29 Data Protection Working Party, Opinion 1/2003 on the storage of traffic data for billing purposes, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp69_en.pdf, 7.

data. They are looking for the proverbial needle in the haystack. And, as *Gore* recently remarked in a speech[24] about the dangers of surveillance, it doesn't help law enforcement to add more hay. Law enforcement needs more timely analysis, not more irrelevant raw data.

But won't that leave copyright owners completely at the mercy of the file sharers? How are they going to be able to enforce their rights if they can't get any IP number records?

Yes. It does. They won't be able to enforce against individual file sharers. Too bad, but removing all Internet privacy just isn't an option. Since the choice is between watching everybody 24 hours a day and lacking efficiency of copyright, my choice is privacy. The copyright holders might choose differently. And they do have some influence on legislation, being able to pay a lot of lobbyists. But we are talking about my opinion here. I will discuss current European law in a moment.

Copyright holders will, however, still be able to follow the money trail.

Anybody who derives a commercial advantage from violating copyrights will need some way to receive funds. The illegal music market in CDs is estimated to have been worth $4.6 billion globally in 2002.[25] Copyright infringement is a large market offline. It would seem to make sense expecting much of that illegal activity to move online in the future. After all, distributing music online is cheaper than producing and moving CDs, leaving larger margins for the copyright violators.

But payment mechanisms on the Internet leave a trail. That is obviously true for the default payment method, the credit card. Nobody can receive credit card payments and stay anonymous. There are some payment systems like e-gold[26] that provide for far superior privacy compared to the default credit card method, but their use is not spread far enough yet.

The situation is similar to that of a spammer who hides the origin of the mail messages behind fake addresses (making the spam message in question illegal under Article 13 paragraph 4 of the telecommunications data protection directive).[27] At some

---

[24] Gore, Al, Freedom and Security, www.moveon.org/gore/speech2.html (November 2003), citing an FBI agent.
[25] BBC news, Global illegal CD market swells, 10 July 2003, news.bbc.co.uk/2/hi/entertainment/3053523.stm.
[26] Gold & Silver Reserve Inc., Gold Itself, Circulated Electronically, www.e-gold.com.
[27] Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002

point, the spammer needs to receive some payment for whatever he is selling. And then, people will be able to locate him.

As a result of my opinion, copyright holders will not be able to enforce their rights against individual file sharers in most cases, since they won't be able to get their names without log files. They will still be able to sue anybody who actually sells illegal copies online. This compromise is similar to what I have proposed[28] as a "no sale doctrine" for awarding damages to copyright holders: Don't award damages if the copyright holder isn't selling the work himself.

And while some file sharers might like the fact that their illegal activity can't be detected easily, there will never be any guarantee of complete anonymity. For example, even if Internet service providers don't keep log files, they might be able to give names while a file transfer is still going on.

Reducing the probability of getting caught by insisting on a minimum privacy standard doesn't remove that possibility altogether. File sharing might be more difficult to prove, but it would still be illegal. Many consumers would probably be happy to pay a reasonable subscriber fee to a legal content provider to avoid even the remote possibility of getting caught. Some of them might even be law-abiding citizens who think respecting copyright is the right thing to do.

2. European Law

My point of view above is only one side of the debate. Many enemies of freedom are working hard on the goal of transforming the Internet into one big surveillance instrument. These enemies of freedom want to watch all citizens at all times. They have no respect for human rights. But they have some power, and they already have scored some success.

The wording of Article 15, Paragraph 1 of the 2002 data protection directive may well be considered a success for the advocates of Internet surveillance. It reads:

" 1. Member States may adopt legislative measures to restrict the scope of the rights and obligations provided for in Article 5, Article 6, Article 8(1), (2), (3) and (4), and

---

concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), europa.eu.int/eur-lex/en/lif/reg/en_register_132060.html.

[28] Lenz, Karl-Friedrich, No Sale Doctrine, k.lenz.name/LB/archives/000449.html#000449 (June 2003).

Article 9 of this Directive when such restriction constitutes a necessary, appropriate and proportionate measure within a democratic society to safeguard national security (i.e. State security), defence, public security, and the prevention, investigation, detection and prosecution of criminal offences or of unauthorised use of the electronic communication system, as referred to in Article 13(1) of Directive 95/46/EC. To this end, Member States may, inter alia, adopt legislative measures providing for the retention of data for a limited period justified on the grounds laid down in this paragraph. All the measures referred to in this paragraph shall be in accordance with the general principles of Community law, including those referred to in Article 6(1) and (2) of the Treaty on European Union."

Under this paragraph, Member States may consider introducing data retention, but they are not obliged to do so. However all measures must be in accordance with the protection of human rights. It must be noted, however, that this is no blanket authority for imposing an obligation to store all "traffic data". Article 15 says "retention of data", not "retention of traffic data". That means that Article 15 opens the door for Internet surveillance legislation at the Member State level, but is far from deciding the issue in favour of the enemies of freedom.

When discussing Article 15, the decision of the European Court of Justice of May 20, 2003 (Österreichischer Rundfunk) needs to be considered.[29]

That decision says in numbers 67 and 68:

"67. However, under Article 13(e) and (f) of the directive, the Member States may derogate *inter alia* from Article 6(1) where this is necessary to safeguard respectively an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters or a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in particular cases including that referred to in subparagraph (e).

68. It should also be noted that the provisions of Directive 95/46, in so far as they govern the processing of personal data liable to infringe fundamental freedoms, in particular the right to privacy, must necessarily be interpreted in the light of fundamental rights, which, according to settled case-law, form an integral part of the general principles of law whose observance the Court ensures (see, *inter alia*, Case C-274/99 P *Connolly* v *Commission* [2001] ECR I-1611, paragraph 37)."

---

[29] snipurl.com/3po9.

This clearly means that any restriction of data protection rights needs to be in accordance with human rights guarantees. Article 15 gives Member States the right to ask for "data retention" only as far as that does not violate the human right of confidentiality of communications.

The Court says in that decision that it can possibly violate human rights standards if data about the income of people working for a television station are made public with their names attached, leaving the final decision of that to the Austrian courts. The purpose of controlling against excessive spending in the public sector doesn't make it necessary to attach any names to income figures.

If that is a potential violation of human rights, watching all citizens at all times for no particular reason is of course completely out of the question. Comparing the case of Internet surveillance with that of Österreichischer Rundfunk, having one's income published seems to be a much less serious intrusion into privacy than having all Internet traffic data recorded.

For the very least this decision of the Court of Justice makes it clear that the human right to privacy needs to be taken seriously.

The latest score in the fight about traffic data is summarized very well by a recent report issued by Privacy International.[30] On page 4 of that report the present situation is summarised:

"Possibly reflecting the altered mindset that led to the proposed Framework Decision, a number of European Member States separately have moved to enact national legislation that similarly would compel the retention of traffic data. These efforts are gathering pace. At least nine of the 15 Member States either have, or intend to enact, legislation calling for mandatory traffic data retention, and the large majority (of) Member States have expressed broad support for an EU-measure calling for mandatory data retention. While authorities in a few states like Germany and Finland remain skeptical, authorities in Greece, Denmark, Austria, Spain, Belgium and most of the rest of Europe are supportive. Where legislation already has been enacted, it typically calls for retention of traffic data for up to 12 months, although at least one Member State has

[30] Privacy International, Memorandum of Laws Concerning the Legality of Data Retention with regard to the Rights Guaranteed by the European Convention on Human Rights, www.statewatch.org/news/2003/oct/Data_Retention_Memo.pdf (October 2003).

set a 3-year retention period."[31]

So it would seem that the enemies of freedom are winning more and more support.

The Commission has said in a recent report that European data protection laws "set some of the highest standards in the world".[32]

That would change radically if mandatory Internet surveillance is enacted. That would mean a complete betrayal of the most important data protection principles. The traditionally "high standards" of European data protection would disintegrate completely, leaving only ruins and fond memories of the good old times when there was respect for human rights in Europe.

On the other hand, the other side is not going down without a fight. There is widespread opposition to Internet surveillance. People are going to challenge any such legislation in court, ultimately in the European Court of Human Rights. Privacy International said in a recent media release:[33]

"Privacy International today warned that it intends to pursue test cases in at least two EU countries where mandatory retention has been implemented. It is currently seeking litigants from within the communications industry."

And, if the enemies of freedom win in court as well as in legislation, there is still another way to preserve anonymous Internet use.

Having log files won't help getting names if Internet service providers don't identify their users in the first place. Wireless Internet access is growing fast. And in many cases, it is provided free of charge and without any registration procedure. That means that wireless Internet access infrastructure has built-in privacy protection.[34]

In that respect it is similar to television and radio. Since television is wireless, there are no records left anywhere about which citizen watched what program. If the enemies

---

[31] See also Statewatch News online, Mandatory retention of telecommunications data would be unlawful, www.statewatch.org/news/2003/oct/26eudataret.htm (October 2003) for more background.
[32] Report from the Commission, First report on the implementation of the Data Protection Directive (95/46/EC), COM(2003) 265 final, europa.eu.int/eur-lex/en/com/rpt/2003/com2003_0265en01.pdf (May 2003), 10.
[33] Privacy International, Media Release, www.statewatch.org/news/2003/oct/26eudataret.htm (October 2003).
[34] See Borland, John, Hot spots elude RIAA dragnet, CNet News.com, news.com.com/2100-1027_3-1026204.html?tag=cd_mh (July 2003).

of freedom wanted to build a large database containing records of all citizens' television usage, that project would be impossible because the wireless nature of the transmission makes sure that there are no such records in the first place. If the Internet moves more and more to wireless anonymous access, any data retention laws would have much less of a damaging impact to privacy interests.

And those opposing Internet surveillance will use this and every other possible technical countermeasure.

So the enemies of freedom might need to ask for outlawing wireless Internet access to make their vision of complete surveillance of all citizens a reality.[35] That won't be easy.

III. Trusted Computing

1. My point of view

Next I will discuss the relation between trusted computing and data protection.

Trusted computing[36] basically removes the control over a personal computer from its owner. Some third party can trust that computer, even when it does not trust the owner of the computer. While DRM is not the only application for trusted computing, it certainly is one that could work much better in a trusted computing environment.[37] Then, on the other hand, as I have noted above already, a recent paper predicts that it might be exactly the other way round, that trusted computing might actually help the file sharers more than the copyright holders.[38]

Removing the control over the computer from its owner is the complete reversal of the original "personal" computer dream on which Microsoft was founded.[39] Taking away control from the owner changes the "personal" computer back into a terminal attached to someone else's network.

---

[35] See Doctorow, Cory and Stross, Charlie, Unwirer, craphound.com/unwirer (June 2003) for one possible vision of a future where wireless Internet access is illegal.
[36] For a good introduction see Schoen, Seth, Trusted Computing: Promise and Risk (October 2003), www.eff.org/Infra/trusted_computing/20031001_tc.php and Bechtold, supra note 2, 633-637. For current developments regarding trusted computing see Bechtold, Stefan, Trusted Computing Blog, cyberlaw.stanford.edu/blogs/bechtold/tcblog.shtml.
[37] Bechtold, supra note 2, 640.
[38] Schechter/Greenstadt/Smith supra note 8.
[39] Gates, Bill, The Road Ahead, 1995, 12.

Many are not happy with that idea.[40]

For example, *Stallman* is opposing trusted computing strongly, calling it "treacherous computing" instead.[41]

Anderson is another influential critic of these proposals. He has published a FAQ on trusted computing.[42]

And *Schneier* concludes a discussion of trusted computing with the words: "My fear is that Pd will lead us down a road where our computers are no longer our computers, but are instead owned by a variety of factions and companies all looking for a piece of our wallet. To the extent that Pd facilitates that reality, it's bad for society. I don't mind companies selling, renting, or licensing things to me, but the loss of the power, reach, and flexibility of the computer is too great a price to pay."[43]

Data protection is all about control of personal data. Trusted computing is all about control of computers. That makes data protection an important aspect when discussing trusted computing.

My position on this:

Trusted computing can coexist with data protection standards. They will be tested, as they have been tested by the development of the Internet, but respect for data protection does not require dumping all plans on trusted computing.

The development of the Internet has lead to many data protection problems. For example, there is the question if the application of European data protection law to websites based outside the EU is possible.[44] There are the problems associated with

---

[40] Against TCPA, TCPA would TAKE your FREEDOM, www.againsttcpa.com/index.shtml is one webpage dedicated to resisting the introduction of trusted computing.

[41] Stallman, Richard, Can You Trust Your Computer? (2002), www.gnu.org/philosophy/can-you-trust.html

[42] Anderson, Ross, 'Trusted Computing' Frequently Asked Questions, Version 1.1, August 2003, www.cl.cam.ac.uk/~rja14/tcpa-faq.html.

[43] Schneier, Bruce, Palladium and the TCPA, August 2002, www.schneier.com/crypto-gram-0208.html.

[44] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Working document on determining the international application of EU data protection law to personal data processing on the Internet by non-EU based web sites, (May 2002), europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp56_en.pdf.

cookies and spyware.[45]

However, even if there are data protection problems, it would not do to ask for killing the Internet because of them.

In the same way, there will be many data protection problems associated with trusted computing. These will have to be addressed and solved in a satisfactory way. They are not so serious as to require abandoning this technology altogether.

The "Trusted Computing Group"[46] is making the most important decisions on the design of trusted computing now. This is an industry standards body composed of private enterprises.

Thompson made an important point about having private enterprises make the important decisions way back in 2002.[47] He said that he doesn't oppose building trusted computing technology as such. Adding security and control is a good idea, considering all the virus and spam problems. However, *Thompson* doesn't want to leave the decisions about the design of trusted computing to private companies. Democratically elected governments should regulate trusted computing.

I agree.

However, that has already happened. There is no need to call the government to the task of regulating privacy regarding trusted computing. There is already a high standard of data protection in force in Europe. These Directives apply to trusted computing just as to every other data processing activity.

The design decisions are now in the hand of private enterprises. Obviously, they have an interest in having people adopt their technology.

Trusted computed won't be successful in the marketplace if privacy concerns are not addressed in a satisfactory way. Many consumers will oppose trusted computing already because it takes away control of their computers from them. If, on top of that, this technology is perceived to invade privacy, nobody will want to use it. Therefore, as one

---

[45] Working Party on the Protection of Individuals with Regard to the Processing of Personal Data, Working document "Privacy on the Internet" - An integrated EU Approach to On-line Data Protection, (November 2000), europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2000/wp37en.pdf.
[46] Trusted Computing Group, Home, www.trustedcomputinggroup.org/home.
[47] Thompson, Bill, Do you trust your computer, BBC News, news.bbc.co.uk/1/hi/technology/2094167.stm (July 2002).

may expect, the "Trusted Computing Group" takes privacy concerns seriously.[48] Which is exactly what *Cohen* has been calling for:[49] Building the new infrastructure with strong privacy protection in the first place is much easier than forcing privacy protection on the technology later on.

A 2002 report of a Canadian Privacy Commissioner gives valuable directions for companies building DRM technology on how to address privacy concerns in an effective way, helping with the task of getting it right in the first place.[50] At this stage, we simply don't know how trusted computing technology will turn out to be built. So I think there is at least some hope that existing European data protection standards will be implemented in the technology. Quite possibly, trusted computing will actually contribute to the development of privacy enhancing technology, as *Microsoft* is claiming.[51]

There is already a recent precedent: The Working Party has discussed with Microsoft the way the Microsoft Passport online authentication scheme is implemented and has reached substantial improvements for data protection.[52] In the same way, one could easily imagine having input from the data protection community into the design of trusted computing. And actually, there is already some substantial such input from German data protection authorities lately. I will discuss this in a moment.

2. European Law

In this section I am going to discuss the requirements of European data protection law for any trusted computing technology, with a special focus on requests from German data protection authorities about the design of trusted computing.[53]

---

[48] Lemos, Robert, Tech giants put chips on security alliance, (April 2003), zdnet.com.com/2100-1105-996032.html.

[49] Cohen, DRM and Privacy supra note 3, part IV "Building Intellectual Privacy into Code".

[50] The Information and Privacy Commissioner/Ontario, Privacy and Digital Rights Management (DRM) – an Oxymoron?, snurl.com/30r4 (October 2002).

[51] England, Paul and Lampson, Butler and Manferdelli, John and Peinado, Marcus and Willman, Bryan (Microsoft Corporation), A Trusted Open Platform, snurl.com/3atk (2003), 59.

[52] Article 29 Data Protection Working Party, Working Document on online-authentication services, europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp68_en.pdf (January 2003).

[53] Entschließung der 65. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 27. bis 28. März in Dresden, TCPA darf nicht zur Aushebelung des

For that purpose, a closer look at what "trusted computing" actually means is necessary, so as to see what kind of personal data are processed in what way. Unfortunately, the specifications[54] are "extremely complex and tersely worded".[55]

According to *Schoen*'s description of the concept,[56] the main features of trusted computing are memory curtaining, secure input and output, sealed storage, and remote attestation. In the following discussion, I assume that readers are familiar with *Schoen*'s introduction to trusted computing features, since I don't have enough space to repeat everything here and I want to focus on the legal implications, rather than the technical concepts.

Memory curtaining is a feature that prevents one program from reading or writing to another program's memory. There seems to be no need to process any personal data for that purpose.

Secure input and output is a countermeasure against keylogger software. If this feature is working, input over the keyboard to one program can't be logged by any other program. As with memory curtaining there does not seem to be any need to process any personal data to achieve this.

Sealed storage is a feature that addresses the problem that people are not able to remember long passwords. A short password easily remembered can be easily broken by trying out all possible variations (brute-force attack). And a long password stored on the hard-drive of a computer doesn't offer any protection if it can be read together with the documents it has been used on.

Sealed storage stops storing passwords. Instead, a password is generated whenever it is needed, based on the software the file was encrypted with and the particular computer.

That feature might imply processing of personal data, as defined in Article 2 a) of the

---

Datenschutzes missbraucht werden, www.lda.brandenburg.de/dsk/dsk65/dsk6502.htm (March 2003); Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (edited by Pfitzner, Roy), TCPA, Palladium und DRM, Technische Aspekte und Analyse des Datenschutzes, www.lda.brandenburg.de/material/tcpa.pdf (June 2003), 22.

[54] Trusted Computing Group, TCG TPM Specification Version 1.2, www.trustedcomputinggroup.org/home (November 2003).

[55] Arbaugh, Bill, Improving the TCPA specification, www.computer.org/computer/homepage/0802/Security/.

[56] Schoen supra note 36.

1995 data protection directive. That definition is:

" a) 'personal data' shall mean any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity; "

Sealed storage means that a file encrypted on an individual user's computer can only be decrypted on that machine, by the particular program that did the encryption.

That means that any file encrypted with this technology can be matched to one individual computer.

If that computer can be matched to one individual user, as with most personal computers, the fact that the encryption establishes a link to the computer means that it establishes a link to one individual user at the same time. That link is "personal data" under European data protection law.

Take this example to explain some more. In the popular "Word" program sold by Microsoft, all documents are tagged with information about the user who wrote them as a default. Many users don't know this. For example, in the debate about introducing the obnoxious and harmful software patents in Europe,[57] FFII claimed that the original Commission proposal was actually written by an lobbyist for the American BSA, since his name appeared in that hidden field, probably without his knowledge.[58]

That example shows that people can be seriously embarrassed if their name is attached as the author of a document and they don't know of that fact. One can easily imagine other situations where this would be very problematic. Therefore, linking authorship of a document to one individual machine and by that indirectly to one individual citizen would seem to mean processing personal data.

d) *Remote authentication* is the most important part of a trusted computing system. Authentication means that unauthorized changes to software can be detected. Remote authentication means that this check can be performed by third parties, not only the computer's owner.

---

[57] Lenz, Karl-Friedrich, Sinking the Proposal for a Directive on Software Patents, k.lenz.name/LB/archives/000264.html (2002).
[58] Foundation for a Free Informational Infrastructure, Introduction, swpat.ffii.org/vreji/papri/eubsa-swpat0202/intro/index.en.html (September 2003).

That means that the computer's owner can prove to those third parties that he is running software that has not been compromised with or without his consent. For example, a content provider like Disney might want to check for the integrity of the software running on a user's computer before allowing that computer to access a video stream. And they would be able to do so because of this feature.

Remote authentication potentially takes away control over the computer from its owner. Most of the criticism against trusted computing[59] is based on this fact.

But what are the implications for the purpose limitation principle of European data protection law? Are there any personal data processed for remote authentication?

The answer to that question depends on the way remote authentication is performed. Trusted computing is by no means a static concept. It develops all the time. The latest version of the specification lists "direct anonymous attestation" as an enhancement to the specification. According to the press release[60] of the Trusted Computing Group, this way of remote authentication does not require the disclosure of personally identifiable information. Again according to the press release, users can generate multiple keys for interaction with different parties to maintain anonymity.

Remote authentication is well known and has been the object of a Directive in 1999[61] as far as the authentication of persons and their electronic signatures is concerned.

Electronic signatures are easily done by public-key encryption technology [62] developed thirty years ago. However, they do need some way of remotely authenticating the relation between a person and her public key. That requires providers of certification services.

Remote authentication of a trusted computing platform also requires interaction with a third party service provider. That is called a "privacy certification authority".[63]

---

[59] Anderson, supra note 42, Stallman, supra note 41, Schneier supra note 43.
[60] Trusted Computing Group, Trusted Computing Group Releases Trustes Platform Module Specification v.1.2 to Enable Enhanced Computing Security, www.trustedcomputinggroup.org/press/news/TPM_release_110503.pdf (November 2003). See also Bechtold, Stefan, TCG 1.2 announced, cyberlaw.stanford.edu/blogs/bechtold/archives/001711.shtml (November 2003).
[61] Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures, europa.eu.int/eur-lex/en/lif/reg/en_register_132060.html.
[62] Wikipedia, Public-key cryptography, en.wikipedia.org/wiki/Public-key_cryptography.
[63] Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht

But the aim of the "privacy certification authority" is exactly the opposite of the certification of a public key by a service provider. In the case of an electronic signature, the authority wants to establish a firm link between a person and an electronic document. That link should be so trustworthy as to be admissible as evidence in subsequent court proceedings. In the case of the "privacy certification authority" with trusted computing, the system wants to avoid establishing a link between a person and a specific trusted computer.

One could as well imagine a trusted computing infrastructure that is built as the existing public key infrastructure, tying every computer to one owner, and making that information available to the public. In that case, running a trusted computing platform would require showing the certification authority a passport, as with the existing certification authorities for electronic signatures. *Stallman*'s science fiction story mentioned above describes such a scenario.[64]

That would be very difficult to sell to a large number of consumers.

The fact that the present specification tries to avoid linking specific users to specific computers is a major success for data protection interests.[65]

No "privacy certification authorities" exist as of now. Therefore no one knows if they can be trusted with the difficult task of adequately guarding privacy interests.[66] This is a difficult task since it presents attackers a single point of failure. In that respect the trusted computing infrastructure is similar to the failed proposals of establishing a "key escrow" infrastructure.[67]

It remains to be seen if these privacy certification authorities will be trustworthy. One of the main requests of German data protection authorities[68] is that users will need to be able to trust third party certification service providers. Specifically, they request that the following problems be solved, noting that a trusted computing infrastructure

---

Brandenburg (edited by Pfitzner, Roy), supra note 53, 13-14.

[64] Stallman, supra note 41.

[65] Bechtold, supra note 2, 636;

[66] Bechtold, supra note 2, 649-650; Der Landesbeauftragte für den Datenschutz und für das Recht auf Akteneinsicht Brandenburg (edited by Pfitzner, Roy), supra note 53, 13-14.

[67] Abelson, Hal and Anderson, Ross and Bellovin, Steven M. and Benaloh, Josh and Blaze, Matt and Diffie, Whitfield and Gilmore, John and Neumann, Peter G. and Rivest, Ronald L. and Schiller, Jeffrey I. and Schneier, Bruce, The Risks of Key Recovery, Key Escrow and Trusted Third Party Encryption, www.cdt.org/crypto/risks98/ (1998), 3.1.3.

[68] Supra note 53.

violating these requests would be unacceptable:

* Users could lose the unconditional control over their own computers to an external service provider.

* Design mistakes or attacks on the external providers could lead to wide-spread loss of functionality for personal computers using trusted computing.

* Third institutions or persons could receive any data about users of trusted computing platforms without their knowledge or consent from central servers.

* The use of personal computers or servers could be restricted as to be impossible without Internet access.

* Access to the Internet or to e-mail could be restricted by software.

* The handling of documents could be restricted by a third party, leading to wide-spread censorship.

* Competition could be restricted, leading to obstacles for the spread of privacy-enhancing open source software.

* Updates could be installed on a user's computer without his consent or knowledge.

To address these problems, the data protection authorities request specifically that users retain the complete control over their own computers. That means that access or changes to a user's computer are possible only after informing the user and obtaining her consent. They also request that users must be able to understand security designs, and that hardware and software can continue to be used without informing third parties of the fact and without the possibility of developing user profiles.

IV. Enforcement Directive Proposal

1. My point of view

The EU Commission has published a Proposal for a Directive of the European Parliament and of the Council on measures and procedures to ensure the enforcement of intellectual property rights[69] in January 2003. This is a very controversial proposal. It

[69] The URL is very long, so I have cut it to: snurl.com/2hqt.

has met with criticism from *Anderson*,[70] *Gross*,[71] and *Hinze*.[72] *Gross* reports[73] that 199 amendments have been proposed. Leading German intellectual property academics[74] have also opposed this proposal.

One of *Anderson's* points in his criticism is data protection. *Anderson* writes:[75]

"Privacy: probably the strongest of the factors undermining privacy, both online and offline, is the increasing importance of price discrimination - see the paper on this subject by *Andrew Odlyzko*.[76] By giving strong legal protection to price discrimination technology, the Directive will increase both the incentives and the opportunities for companies to price discriminate in ways likely to be privacy-invasive."

I don't share these privacy concerns.

Anderson agrees with *Odlycko*'s position[77] that the desire to implement price discrimination will lead to erosion of privacy. I am neutral on this point. Quite possibly, price discrimination makes sense for many business decisions. This might by a factor in reducing privacy.

But *Anderson* then says: The draft directive gives strong legal protection for price-discrimination technology. That will lead to added privacy costs.

I hesitate to agree unconditionally with that concern.

The starting point for examining the "strong legal protection for price-discrimination

---

[70] Anderson, Ross, The Draft IPR Enforcement Directive – a Threat to Competition and Liberty (2003), www.fipr.org/copyright/draft-ipr-enforce.html.
[71] Gross, Robin, IP Justice White Paper on Proposed European Union IP Enforcement Directive, Europe's Proposed Intellectual Property Directive Unmasked – Overbroad Proposal Threatens Civil Rights, Innovation and Competition (2003), www.ipjustice.org/ipenforcewhitepaper.shtml.
[72] Hinze, Gwen, The EUCD and the DMCA in 2003: How Legal Protection for Technological Measures is shaping Consumers' and Copyright Owners' Digital Rights (2003), www.upgrade-cepis.org/issues/2003/3/up4-3Hinze.pdf.
[73] Gross, Robin, Fortou Proposes EU Law to Send European P2P File-Sharers to Prison, Urges Controversial Amendment to Intellectual Property Enforcement Directive (October 2003), ipjustice.org/code/update102403.htm.
[74] Drexl/Hilty/Kur, Vorschlag für eine Richtlinie über die Maßnahmen und Verfahren zum Schutz der Rechte am geistigen Eigentum – eine erste Würdigung, GRUR 2003, 605-606.
[75] Anderson, supra note 70.
[76] Odlyzko, Andrew, Privacy, Economics, and Price Discrimination on the Internet (July 2003), www.dtc.umn.edu/~odlyzko/doc/privacy.economics.pdf.
[77] Supra note 76.

technology" is Article 21 of the proposed directive.

Unfortunately, at the present time (November 2003) there are only drafts. We will have to wait and see if any directive will be adopted. And what the final version of Article 21 will turn out to be, if the proposal is adapted against many critical voices.

I will discuss the question based on the original Commission proposal of January 2003[78] and the Draft Report of the European Parliament Committee on Legal Affairs and the Internal Market by *Fortou*.[79]

In the original proposal, the wording of Article 21 is:

"1. Without prejudice to particular provisions applicable in the field of copyright, related rights and the sui generis right of the creator of a database, Member States shall provide for appropriate legal protection against the manufacture, import, distribution and use of illegal technical devices.

2. For the purposes of this Chapter,

(a) "technical device" means any technology, device or component which, in the normal course of its functioning, is designed for the manufacture of authentic goods and the incorporation therein of elements which are manifestly identifiable by costumers and consumers and which make it easier to recognise the goods as being authentic.

(b) "illegal technical device" means any technical device which is designed to circumvent a technical device which permits the manufacture of goods infringing industrial property rights and incorporating manifestly identifiable elements described in point (a)."

Where does this Article 21 give strong legal protection to price-discrimination technology?

In my view, the goal of Article 21 is to protect technology that enables consumers to recognise authentic goods. For example, if someone sells wristwatches under an expensive brand, they might incorporate some kind of technology enabling costumers to make sure that the watch they are buying is not counterfeit.

Article 21 would protect this technology.

---

[78] Supra note 69.
[79] Committee on Legal Affairs and the Internal Market, Rapporteur: Janelly Fortou, available at the shortcut URL snurl.com/2kkl (October 2003) at point 6.

Of course, there is some protection for price discrimination concerned here. The only reason many costumers pay thousands of Euros for a branded wristwatch when they could get a completely functional watch at a fraction of the price is that they want to impress other people with the expensive brand. So the trademark as such is a powerful tool for price discrimination.

However, the technology protected in Article 21 adds nothing to this.

For example, under European trademark law, trademarks can not be used for price discrimination between different member states. Under Article 7 of the trademark directive[80] the owner of a trademark can not use it to prevent a French wholesaler to sell trademarked goods to Germany, if he has sold these goods to the French wholesaler in the first place (exhaustion).

And technology protected under Article 21 would not change anything.

There is no way a trademark owner could use Article 21 technology as a technical means to achieve price discrimination excluded by Article 7 of the trademark directive. All the technology does is to protect the trademark owner against counterfeiting.

But in the case of counterfeit goods, the exhaustion principle in Article 7 of the trademark directive doesn't apply in the first place. It only applies for goods which have been put on the market by the proprietor of the trademark.

So I don't really see why Article 21 of the original proposal would protect price-discrimination technology and pose a threat to data protection.

Article 21 has seen a major modification in the Draft Report of the European Parliament Committee on Legal Affairs and the Internal Market by *Fortou*.[81] In the wording of that Draft Report the proposal now is:

"1. For the purpose of this Article, "technical device" means any technology, device or component designed to be applied to tangible products protected by an intellectual property right to facilitate the detection of counterfeit goods. "Illicit technical device" means any technology, device or component which misleads, is designed to deceive or is likely to mislead any person as to the authenticity of the tangible products concerned.

2. Member States shall provide for appropriate legal protection against:

---

[80] First Council Directive 104/89/EEC of 21 December 1988 to approximate the laws of the Member States relating to trade marks, OJ L 40, 1.
[81] Supra note 79.

(a) the manufacture, import, distribution, sale, hire, advertising for sale or hire, possession and use of illicit technical devices;

(b) the import or distribution of tangible products to which illicit technical devices have been applied or whose technical devices have been removed, tampered with or disabled;

(c) the application, on products that infringe intellectual property rights, of technical devices designed from the outset to be used by right-holders on authentic products;

(d) the act of removing, tampering with or disabling technical devices or circumventing them.

3. This Article shall apply to the technical devices applied to tangible products in the sense of physical objects, including their packaging, and not to digital goods. This Article shall be without prejudice to the provisions applicable in the area of copyright, associated rights and the sui generis rights of the manufacturer of a database.

4. Right-holders shall remain free to use technical devices within the meaning of this Article."

This wording is much longer than the original proposal. And it contains substantially more prohibitions in paragraph 2. The prohibitions in paragraph 2 d) are unnecessary and confusing, especially the prohibition against circumvention.[82]

However, even with the arguably substantially broader new proposal, Article 21 would still basically only protect technology that “facilitates the detection of counterfeit goods”. It is still not clear how price-discriminating technology should be protected under this wording.

And in the new wording Article 21 would be applied only to tangible products, leaving the protection of copyrighted works against counterfeiting completely to the Articles 6 and 7 of the 2001 copyright directive.[83]

Let’s try to imagine some kind of price-discriminating DRM technology. For example, an online seller of music files might give listeners 15 years and younger a 95 percent

---

[82] Lenz, Karl-Friedrich, Enforcement Directive, k.lenz.name/LB/archives/000640.html (October 2003).

[83] Directive 2001/29 of the European Parliament and of the Council of 22 May 2001 on harmonisation of certain aspects of copyright and related rights in the information society, OJ L 167, 10.

discount, figuring that they would just use illegal downloads without that. Obviously, that vendor would need some way to make sure who is buying a subscription and how old that person is. So they would need personal data. And some DRM technology might be built to enable the price discrimination.

In the Draft Report Article 21 wording, this DRM technology would not be protected because it is not about tangible goods. And even under the original proposal the technology would not be protected since it is not about authentication. Anyone breaking the technology and succeeding in getting a 95 percent discount even if they are already 45 years old would not circumvent technology that "makes it easier to recognise the goods as being authentic". The person breaking the DRM technology would know that they are getting authentic files at the lower price.

2. European Law

Even if Article 21 of the proposal in the wording finally approved would "raise the incentives and opportunities" for privacy invasion, that would not mean that the existing European data protection legislation[84] would be overruled.

For example, Article 9 of the proposal gives intellectual property right holders a claim to information about producers and distributors of infringing goods. The Draft Report[85] adds an exception to this right in paragraph 3: "Paragraphs 1 and 2 shall apply without prejudice to other provisions which: (da) govern the protection of natural persons with regard to the treatment of data of a personal nature"

So clearly the proposal does not intend to water down the existing European data protection legislation. The Commission says about the 1995 data protection Directive that "the Directive itself sets out some of the highest data protection standards in the world".[86] That might be open to debate. However, there definitely is a strong data protection framework in place. And the enforcement directive proposal does not modify that in any way.

---

[84] Commission, Data Protection: Legislative Documents, europa.eu.int/comm/internal_market/privacy/law_en.htm.
[85] Supra note 79.
[86] Report from the Commission, First report on the implementation of the Data Protection Directive (95/46/EC), supra note 32 (May 2003), 10.