Robotik und Recht 15

Eric Hilgendorf/Jochen Feldle (eds.)

Digitization and the Law

Nomos

Robotik und Recht

Edited by

Prof. Dr. Dr. Eric Hilgendorf, Universität Würzburg
Prof. Dr. Susanne Beck, LL.M., Universität Hannover

Volume 15

Eric Hilgendorf/Jochen Feldle (eds.)

Digitization and the Law

Nomos

The Deutsche Nationalbibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data are available on the Internet at http://dnb.d-nb.de

ISBN 978-3-8487-4700-9 (Print)
978-3-8452-8930-4 (ePDF)

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

ISBN 978-3-8487-4700-9 (Print)
978-3-8452-8930-4 (ePDF)

Library of Congress Cataloging-in-Publication Data
Hilgendorf, Eric / Feldle, Jochen
Digitization and the Law
Eric Hilgendorf / Jochen Feldle (eds.)
140 p.

ISBN 978-3-8487-4700-9 (Print)
978-3-8452-8930-4 (ePDF)

1st Edition 2018

Preface

The present volume brings together the contributions presented at the 5th Würzburg Conference on Technology Law on May 5th and 6th, 2017. The event was devoted to legal comparison between Germany / Europe and the USA, and was the prelude to the founding of a German-American working group, which will be specially dedicated to technology law in the United States and Europe.

Special thanks go to Roger Fabry for his excellent linguistic support.

Wurzburg, December 2017

Eric Hilgendorf
Jochen Feldle

Table of Contents

Introduction: Digitization and the Law – a European Perspective

Eric Hilgendorf[*]

I. New Technologies and their Convergence

"Digitization of information" means, to state it in the simplest way possible, the representation of information as a sequence of zeros and ones. Digitized information can be edited, stored and easily transferred between computers. In view of the high power of today's computers and their global networking via the Internet, this means that vast amounts of information can be processed, stored and transmitted in real time.

A second characteristic need also be considered: Digitized information is enormously plastic. Texts, pictures, video and audio files can be converted into digitized form. Until recently, these kinds of information could only be perceived by means of monitors, loudspeakers, or, respectively, headphones. At the present time, a new breakthrough is emerging under the keyword "virtuality", meaning a significantly more intensive form of experience which is digitally-based. The creation of virtual environments is making extremely rapid progress so that it will soon be possible to "dive into" deceptively real artificially created environments using data goggles.

The "digital revolution" is happening at the same time as other technological developments. One worth mentioning are the enormous advances in microphone technology, which make it possible for us to record much more data, and then also at much higher levels of quality, than was ever previously possible. In this context, one has referred to the new granularity, or fineness, of data.

Perhaps even more far-reaching are new forms of autonomous systems, i.e. technological systems, which react independently of human input to new factual situations and can thus successfully deal with unforeseen problems autonomously. Such systems are to a certain extent already regarded as independent actors. It can be assumed that their importance will increase significantly in the near future. This development is particularly

---

* Prof. Dr. Dr. Eric Hilgendorf, Julius-Maximilians-Universität Würzburg.

controversial because these technological systems are increasingly able to learn for themselves, that is, to expand their knowledge base independently as a product of experience.

II. The Digital Revolution and the Law

What does all of this mean for the law? In order to shed light on the impact of digitization on the legal system and its stakeholders, the following six topics should be considered (1) legal resources, (2) the application of the law, (3) legal policy, (4) programming and concomitant algorithmization of the law, (5) the representation of law, (6) the resulting consequences for the perception and acceptance of the law, and finally (7) more far-reaching social and political consequences.

(1) New Tools and Methodologies in the Law

It can be said without exaggeration, that there has been a revolution in the technological and informational resources available to lawyers which can be subsumed under the catchphrase "from statute book to networked computer". Text editing on personal computers has now become a matter of course. The same can be said for research using computers, for example, in legal databases online or offline. In this context, the use of legal precedents or boilerplate clauses is, in many respects, not without problems. It must be obvious that these lawyering tools not only bring advantages, but also raise questions. Sections of text written by someone else can easily be included into a document without making them recognizable as quotations; also among digitally socialized academics, borrowing footnotes from other works via "copy and paste" has become widespread.

The implications of these developments for legal texts, such as student assignments, academic articles, decisions by administrative authorities or written dispositions by the prosecution in criminal proceedings, are still unclear. These changes in lawyering resources and methods and their effects on legal thinking deserve more attention than they have been given up to now. This includes the old question of whether computers with appropriate software can make legal decisions, an idea which has long been under discussion in legal methodology, but which now appears for the first time to be technically feasible on a large scale.

(2) Application of the Law: Can it Accommodate the Change?

As a result of the digital revolution which is affecting many aspects of the way we live and work, involving many fields of human activity, the question emerges as to the extent to which existing legal norms are or will be applicable to facts arising in the context of digitized situations and circumstances. Thus it could be a question for discussion, for example, whether a purchase agreement (i.e. a kind of contract) under § 433 German Civil Code (*Bürgerliches Gesetzbuch* – BGB) can be concluded by e-mail. In point of fact, this question was answered years ago. In the criminal law, the problem arose as to whether data were protected by § 303 German Criminal Code (*Strafgesetzbuch* – StGB), i.e. whether the deletion of data constituted the offence of criminal damage. This was rejected by prevailing legal opinion, so in 1986 the German Parliament adopted § 303 a and § 303 b of the Criminal Code as part of the Second Law to Combat Economic Crimes (white collar crime) in order to close this lacuna in the law. Another issue under discussion, for example, was the extent to which mass emailings (spam), such as those sent for advertising purposes, could be criminalized, but that was ultimately rejected. In the first criminal law example above, digitized information was the thing destroyed (the object of the crime); in the second it was the means of committing the offence.

There are crimes that have already existed for a long time in the analog world, but now, in the digital world, these offences are becoming more common than they ever were previously. The Internet provides ready opportunities to spread hate messages, or engage in cyber-mobbing, trolling and the like. Moreover, the new communications possibilities afforded by the internet are facilitating the commission of offences by helping to bring perpetrators and victims together. A somewhat macabre example of this are the cases of consensual cannibalism, which had previously been difficult to carry out due to the difficulty of establishing contact with like-minded people; the chance that two people with such extreme proclivities would meet in the analog world were extremely small. Nowadays, it has become much easier to search for correspondingly inclined partners via the Internet; sometimes reference is even made to "cannibal networks".

Public law is also being subjected to not inconsiderable pressure to adapt to changing circumstances. One example is the extension of the protection of fundamental rights, such as the "right to informational self-determination". This right was recognized in 1983 in the German Federal Constitution Court's landmark decision in the *Census Act Judgment* (*Volk-*

szählungsurteil). Another example concerns the question of whether and to what extent public authorities can undertake official administrative measures via the Internet. The German Parliament tried to regulate this area through the E-Government Act (2013), but the implementation of this statute is considered by many to have lagged behind expectations.

The advancing digitization of our entire life and work environments means that in some areas completely new questions have emerged. The ubiquitous networking of things in the "Internet of things", the ever more efficient handling of cumulative data (big data) and, finally, the development of augmented reality or virtual reality, are all amongst the most important trends in technology at present. These developments raise significant legal questions, from the curbing of impending new forms of cybercrime, through data protection, to the question of the application of the law to avatars, that is, to artificial figures in virtual space. It should also be noted that among these questions some questions are also rather exotic, including whether robot prostitution is legal, or questions about digital legacies, or even whether someone, in contemplation of death, can perpetuate himself in the form of a computer program (RIP: Rest in Pixels).

(3) Legal Policy

If the applicable law can no longer be extended and applied to new technological developments, it will be parliament‘s task to settle the new questions by passing new legislation. Law and legal policy are therefore closely linked. Given the speed with which the digital revolution is taking place, it is not surprising that in almost all areas of the law, *lege lata* is facing challenges. Thus, for example, new forms of socially harmful behavior such as "identity theft" are emerging on the Internet, which confront both tort law as well as the criminal law.

Again and again, the question has been raised whether there is a need to legislate new criminal offences, such as the digital trespass to property, or for increased penalties for the offence of insult (*Beleidigung*), when it is committed via the Internet. Discussions are taking place in the civil law as to whether autonomous systems should be subjected to a strict liability regime in tort; making tortfeasors liable for damage regardless of fault has proved itself, for example, both in the context of railways and automobiles. Another primarily civil law issue is the question of whether a quasi-property right should be created in (particularly non-personal) data, an is-

sue that is becoming more and more important as a result of the rapidly growing commercial value of such data.

Facing such challenges, technology law is confronted with three tasks: (1) Advising legal practitioners, i.e. lawyers, public prosecutors and judges; (2) Advising legal policy makers, i.e. the legislature, for example via publications, through participation in advisory bodies, or through activities as experts; (3) Advising the engineers themselves who develop new technology. The goal is to ensure, by taking compliance measures, that clashes between technology and the law never occur. In this context, it is also necessary to provide engineers with a certain level of basic education in law, for example, a basic understanding of how civil liability works in our legal system.

(4) From Programming to the Algorithmization of the Law

An interesting special problem is the programmability of law (i.e. whether it can be transposed in computer code instructions which a machine can follow and execute). Automation is leading to increasing demand for machines which perform their functions in accordance with the law. Thus autonomous systems used in stock market trading must, in principle, be in a position to comply with applicable legal norms. Autonomous vehicles which drive on public roads must follow the rules contained in the road traffic code, and robots, which are in particularly close contact with human beings, need to have internalized “moral and legal codices”, which, among other things, ensures that the machines do not harm the humans they interact with.

All these problems raise the question of how machines can be informed about all these legal requirements. In principle there are two possibilities: (1) The transmission of legal information comes from outside, for example via the infrastructure of the roads on which the autonomous vehicles are moving; (2) "legal instructions" are contained within them, i.e. by programming them with legal rules. However, each programming of legal rules requires that not only the rules but also the application of the rules in specific cases must be transposed and transmitted in computer language, i.e. as algorithms.

Algorithmization of the law leads to a new and compelling need to explicate the law: legal decisions, the premises and reasoning of which, within the framework of traditional methods of applying the law, were of-

ten vague and approximate, must now be analyzed and presented with great precision. A good example of this is a well-known dilemma discussed in the context of automated vehicle transport: a vehicle is approaching an accident scene at high speed: three people are lying unconscious on the road, one person has been able to drag himself to the roadside and is leaning against a signpost. A human driver would not be able to swerve to avoid a collision and would run over the three people lying on the ground.

An autonomous vehicle, on the other hand, has powerful sensors and a fast on-board computer and is thus able to swerve to avoid running over the people on the road. Unfortunately, it would then collide with the person leaning against the signpost. How should the algorithm for the on-board computer be programmed? Such problems have hitherto been quite relevant in theoretical discussions, one example of which is the well-known *switchman problem*. The automation of road transport means that we have to make the rules that should apply in such situations explicit, and then program the vehicles accordingly.

This is often anything but simple. Suppose an automated vehicle, on a narrow street, is approaching a group of three children, who have suddenly jumped onto the road. One child is running ahead of the two others. The children are located on the road so that one child will be hit by the left fender of the vehicle, and the other two by the right fender. If the trajectory of the vehicle does not change, all three children will be struck by it and injured or killed. The vehicle, of course, can be steered slightly to the right or to the left, so that not all the children will get run over. If it is steered to the left, one child will be struck. If it is steered to the right, two children will get hit.

Intuition tells us that it should be steered to the left in order to minimize the number of victims. That solution would mean, however, that human lives would be quantified and weighed against each other. Can that be justified? The example shows how technological development, and the explication pressure associated with it, can call into question our established ways of thinking and reacting.

From the perspective of legal theory, one very interesting question is how the pressure to explicate will affect legal drafting and argumentation. In order to be represented in algorithms, the relevant aspects of a problem must be identified as precisely as possible and the logical relationships between the elements must be elucidated. A simple "balancing" as is widespread in some areas of fundamental rights law, for example, would

not meet these requirements. The necessity of making key arguments comprehensible to the computer, therefore, leads to pressure towards being more precise, a phenomenon which might possibly have salutary effects in some areas of legal science.

(5) New Ways of Disseminating and Consuming Legal Content

As the Internet has developed, new sources of legal information have also emerged. One of the most important of these is the internet encyclopedia *Wikipedia*. It contains information on almost all legal issues, often at very high levels of sophistication. Without effective quality control, Wikipedia would never have been able to drive established encyclopedias such as *Brockhaus* or *Enzyclopaedia Britannica* out of the market.

The existence of internet-based sources of legal information means that this information is now much more readily available than ever before. Trips to the library have to a large extent been replaced by typing in keywords or making swiping movements on a smartphone. Something that is particularly noteworthy is that information on foreign legal provisions is, in principle, as easy to obtain as information on German law. This is a major difference from the situation in the past, when at best big university libraries contained holdings on foreign law.

A second point that characterizes today's situation is that the boundaries between professionally solid treatments of the law, popular representations and so-called "fake news" are beginning to blur. This has important implications for the trust that users place, or at least ought to place, in legal resources on the Internet. The availability of more information therefore does not necessarily lead to improved certainty about finding out what the law on a given issue actually is. The opposite might even be the case today.

In addition, the Internet has brought new opportunities and incentives for engaging in legally binding commercial transactions. For example, contracting can be done very easily via the Internet. It is obvious that this may pose new challenges for consumer protection. Communication on the Internet highlights some typical psychological idiosyncrasies of normal users, which also have legal relevance. For example, use of the Internet, especially at home, gives users a sense of privacy, i.e. a feeling of not being observed, which is exactly the opposite of what is really happening. There is scarcely an area of human activity that is so relentlessly moni-

tored as behavior on the Internet. The feeling of privacy, in contrast, often leads to a loss of inhibitions, with users forgetting that they need to exercise well-practiced self-control behaviours. There is therefore hardly a place where one's "privacy" is potentially exposed to more serious invasions than when surfing the Internet on a home computer.

The control of Internet content is hardly possible. Control of what is placed on the Web 2.0 is particularly difficult, since users can put their content online themselves. It follows that the possibilities for controlling legal content on the Internet are very limited. Discussions are currently under way as to whether in might be possible to carry out some kind of control of the truth of content on the Internet. This could be done by people who examine the content, but also by machines that check the plausibility of content. The latter would have the advantage that far more content could be examined. Whether such content control is desirable, however, and who should decide on the truth or falsehood of the content, is still an open question.

Another way to prevent the uncontrolled proliferation of both false and accurate legal information on the Internet would be the increased involvement of governmental authorities, which could publish relevant information on the Internet. This is already happening on a large scale and at high levels of quality. Good examples are the information pages of German federal and state government ministries. Furthermore, there are numerous examples of the successful publication of legal content by local government authorities on the Internet, namely on their e-government websites.

That is enough said in respect of publishing traditional legal texts on the Internet. The use of the Internet is also leading to the representation of law in new and non-traditional ways. Frequently, legal texts or texts with legal content are accompanied by audio or video files.

A particularly significant application of these new ways of publishing legal content are new methodologies for teaching law such as e-learning. The combination of text, audio and video leads to inclusion; even people with lower levels of education can be reached through video sequences and thus be sensitized to legal problems. Thus new ways of publishing legal content should in principle be deemed as positive. Nevertheless, popularizations of the law can also result in trivialization and ultimately lead to a loss of respect for legal rules.

In this context, it may be helpful to search our cultural history for other forms of not exclusively text-based transmission of legal content. Such material is easy to find. The treatment of legal problems by actors goes all

the way back to court dramas written in antiquity (just think of the Sophocles' play *Antigone* written ca. 440 BC). Since the invention of cinema and television, there have again and again been important feature films, which have made legal content accessible to wider audiences, including *12 Angry Men* (1957), *Inherit the Wind* (1960), *To Kill a Mockingbird* (1962), and *Erin Brockovich* (2000). Such works have probably played a significant role in the development of legal consciousness and legal knowledge in their viewers. There is also much evidence that the adversarial form of court procedure characteristic of common law legal systems has been given currency worldwide mainly through Hollywood films. The digitizability and consequent internationality of all content, and thus also of legal content, suggests that in the future there will be significantly more audio content and video content, but above all also many more legal offerings in virtual reality.

A very interesting new way of presenting legal content is the visualization of law. Images can have quite different effects – and thus also have: different functions. First of all there are aesthetic effects, that is, the embellishment of legal information through images. However, images are used much more frequently to illustrate or explain legal content. An easily overlooked issue here is the defamiliarization, which visual representations can cause. As a result, they can, like hardly any other medium, encourage viewers' reflection on the law.

Finally, the fourth possible function of images in law is criticism: pictorial representations can be used in an outstanding way to represent particular situations, or even lawyers, in a critical light. A famous example of this are Daumier's socially-critical caricatures of lawyers. Finally, photographs can also be put into the category "criticism through pictures", such as those which represent untenable legal situations.

The development of the Internet means that many more images referring in some way to the law are available today than in the past. The social consequences of this visualization have not yet been adequately considered.

(6) The Consequences of Digitization for the Perception, Acceptance and Functioning of the Law

Until the twelfth century law was transmitted orally. Law that was handed down in this way was hardly suited to be used as a mechanism for the ex-

ercise of power on a nationwide basis, because its content and its interpretation depended on those who recited it to the public. Also, possibilities for making changes in the law were very limited. Legal science as we know it today did not exist. After Roman law was rediscovered, there was a shift from orality to literality, i.e. from oral transmission of the law to written transmission of the law. Unlike oral law, written law was extremely well suited for the exercise of sovereign power. Subsequently, European legal science emerged, which devoted itself to the collection, interpretation, systematic presentation, and ultimately to the further development of the body of law which had previously been handed down orally.

It is not without allure to ask whether we are today at the threshold of a transition from liter-ality to the digit-ality of the law. It has been shown above how new digital communication and presentation technologies are fundamentally altering our approach to the law. What does this mean for the acceptance of law by the populace? What are the social and political consequences of this development? And what will the effects be for legal science?

(7) Societal and Political Consequences

The Internet also has social consequences, which are real rather than theoretical. There is much evidence that the increasing digitalization of our workflows and their automation will lead to huge losses of jobs. Internet communication offers new possibilities of manipulating the population. A danger that is already looming on the horizon is the potential loss of the ability of humans to solve problems on their own, as a result of the automation of problem-solving.

It is doubtful whether the law alone will be able to cope with all of these consequences. One of the traditional tasks of law is the creation of legal certainty. But can this still be guaranteed at a time when almost any legal content is available on the Internet? All in all, the question arises as to how much digitization we can afford to achieve. What is certain is that the process of digitization must not be accepted passively, but rather must be steered. The means for this control is the law. The key issue is to ensure that the fundamental guiding principles of our legal system, such as the rule of law and the orientation towards human dignity and human rights, will continue to be preserved in the future.

III. Summary and Outlook

If we try to summarize the new tasks of legal science, which have been posed by digitization, the following picture emerges: The law first of all faces the task of bringing the new technologies and the law into harmony. This can be achieved by adapting the law to technology, but also by adapting technology to law. Another important present task is the management of new forms of socially harmful behavior through the introduction of appropriate forms of criminal liability and criminal law.

The algorithmization of law is leading to a new compulsion to explicate, because the law needs to be translated into computer-compatible language. Such tasks are already being faced today, for example, in the field of road traffic law, where the programming of traffic signs is being discussed. In the medium term, the task will be to program legal rules into the on-board computers of autonomous vehicles. Another major problem related to the algorithmization of law is the analysis and assessment of dilemma situations in road traffic, where autonomous vehicles will face very difficult decisions on how to maneuver during road traffic accidents.

All of these are major legal challenges that lawyers can hardly cope with by themselves. What is therefore required is a reflected interdisciplinarity which in particular aims at exploiting empirical findings made by the natural sciences. Lawyers have hardly ever up to now received training in interdisciplinary work methods; the linguistic difficulties they have in dealing with professionals from other disciplines are virtually proverbial. There is much to be said for devoting more attention to the digitization of law in German legal education than has hitherto been the case.

Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*

Sara Sun Beale# *and Peter Berris*+

Introduction

This is the age of the "Internet of Things," (IoT) where "everyday objects... connect to the Internet and... send and receive data."[1] The lines between computers and humans have blurred as "[t]he Internet now affects the world in a direct physical manner."[2] The Federal Trade Commission predicts that more than fifty billion devices will be part of the IoT by 2020,[3] including items ranging from kitchen appliances to Fitbits and heart monitors.[4] As Bruce Schneier explained to Congress, "everything is

---

* For a revised and extended version of this project, see Sara Sun Beale & Peter Berris, *Hacking the Internet of Things: Vulnerabilities, Dangers, and Legal Responses*, 16 Duke L. & Tech. Rev. 161 (2018) (examining reasons for vulnerability of IoT and how current legal system responds, discussing practical and legal barriers to investigation and prosecution of hacking, and evaluating the merits and pitfalls of hacking back against botnets from legal, practical, and ethical standpoints).

Charles L.B. Lowndes Professor, Duke Law School.

+ J.D., Duke Law School, 2017.

1 Federal Trade Commission, internet of things: Privacy & Security in a Connected World i (2015), available at https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127IOTrpt.pdf.

2 *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statement of Bruce Schneier), [hereinafter "Schneier"].

3 Christina Scelsi, *Care and Feeding of Privacy Policies and Keeping the Big Data Monster at Bay: Legal Concerns in Healthcare in the Age of the Internet of Things*, 39 Nova L. Rev. 391, 396 (2015).

4 Andrew Meola, *What is the Internet of Things (IoT)?*, Business Insider, (Dec. 19, 2016), http://www.businessinsider.com/what-is-the-internet-of-things-definition-2016-8.

now a computer."[5] The reach of the IoT extends beyond consumer goods to major items and infrastructure components including cars, airplanes,[6] hospitals, telecommunications networks, and power grids.[7] As a result, "insecurity" in the IoT "puts human safety at risk."[8] Moreover, in the age of the IoT, the actions of "hackers" may carry physical consequences.[9]

This paper proceeds as follows. Section I describes episodes in which the IoT has already been hacked as well as the potential for other attacks, and Section II examines the reasons for the vulnerabilities that facilitate hacking. Section III explores how criminal law now responds to attacks on the IoT, and Section IV concludes with a discussion of legal reforms that might reduce the current vulnerabilities and prevent future attacks.

I. Threats and Vulnerabilities

A. How the IoT has been hacked

On October 21, 2016, major websites, including Netflix, Twitter, Reddit and the New York Times, were inaccessible for up to several hours.[10] The interruption was the result of a Distributed Denial of Service attack ("DDoS")[11] against the company Dyn, which "is one of many outfits that

---

5 *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript): *Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 27 (2016) (testimony of Bruce Schneier), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf [hereinafter "Schneier Testimony"].

6 *Id.* at 29.

7 *Id.* at 57.

8 *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statement of Kevin Fu), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-FuK-20161116.pdf [hereinafter "Fu"] (warning the HECC that "the Dyn attack is a sign of worse pains to come").

9 *See* section I, *infra*.

10 Nicole Perlroth, *Hackers Used New Weapons to Disrupt Major Websites Across U.S.*, N.Y. Times, Oct. 21, 2016, at https://www.nytimes.com/2016/10/22/business/internet-problems-attack.html?_r=0 [hereinafter "Perlroth"].

11 A DDoS is when "an attacker attempts to prevent legitimate users from accessing information or services. . . . [such as] when an attacker 'floods' a network with information. . . . The server can only process a certain number of requests at once, so if an attacker overloads the server with requests, it can't process [legitimate re-

host the Domain Name System, or DNS, which functions as a switchboard for the internet."[12] The perpetrators of the Dyn attack exploited "a vulnerability in large numbers—possibly millions—of... devices like webcams and digital video recorders" and used them as a botnet[13] to flood Dyn with traffic.[14] This "attack traffic" combined with "legitimate traffic" to overwhelm Dyn,[15] taking down "dozens of websites" with it.[16]

Despite the large scale of the interruption, the Dyn attack has been characterized as "benign" since it did not result in physical injury or property damage.[17] Nevertheless, it underscored the risk that the next attack may be devastating.[18]

In response to the Dyn attack, the House Energy and Commerce Committee (HECC) held a hearing to address the threats posed by hacking in the IoT.[19] Expert testimony was grave. Bruce Schneier warned that "the internet is now dangerous...."[20] Dr. Kevin Fu told the HECC that he "fear[s] for the day where every hospital system is down, for instance, be-

---

quests]. This is a 'denial of service' because you can't access that site." Mindi McDowell, *Security Tip (ST04-015) Understanding Denial-of Service Attacks*, US-CERT, Feb. 6, 2013, https://www.us-cert.gov/ncas/tips/ST04-015.

12 Perlroth, *supra* note 100.

13 A botnet is a "collection of computers compromised by malicious code and controlled across a network." *Glossary*, US-CERT, Jan. 11, 2017, https://niccs.us-cert.gov/glossary#B. Although they can be used for collaboration, "botnet" is a pejorative term. Zach Lerner, *Microsoft the Botnet Hunter: The Role of Public-Private Partnerships in Mitigating Botnets*, 28 Harv. J.L. & Tech. 237, 237–38. (2014) [hereinafter "Lerner"].

14 Schneier, *supra* note 2, at 2.

15 Scott Hilton, *Dyn Analysis Summary of Friday October 21 Attack*, Dyn: Vantage Point, Oct 26, 2016, http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/.

16 Schneier, *supra* note 14.

17 *Id.* at 3.

18 *See* Fu, *supra* note 8, at 2.

19 *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript): *Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 4–5 (2016) (statements of Greg P. Walden, Chairman, Subcomm. on Commc'n & Tech.), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf.

20 Schneier Testimony, *supra* note 5, at 59.

cause an [IoT] attack brings down the entire healthcare system."[21] Dale Drew cautioned that the culprits of the Dyn attack relied on "just a fraction of the total available compromised [IoT devices]... demonstrating the potential for significantly greater havoc...."[22]

Illustrations of the dangers abound. Many prominent examples of hacking in the IoT pertain to automobiles.[23] In 2015, Fiat Chrysler recalled 1.4 million cars in response to a widely publicized demonstration where hackers took control of a Jeep Cherokee through its infotainment system.[24] They were able to "turn the steering wheel, briefly disable the brakes and shut down the engine."[25] In 2010, the disgruntled former employee of a

---

21 *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript): *Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 43. (2016) (testimony of Kevin Fu), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf [hereinafter "Fu Testimony"].

22 *Understanding the Role of Connected Devices in Recent Cyber Attacks: Hearing Before the H. Comm. on Energy and Commerce*, 114th Cong. 3 (2016) (statements of Dale Drew), http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Wstate-DrewD-20161116.pdf [hereinafter "Drew"].

23 Automobiles are an obvious target for hackers because they can cause physical damage, *and* because they are vulnerable. *See* Cheryl Dancey Balough, Richard C. Balough, *Cyberterrorism on Wheels: Are Today's Cars Vulnerable to Attack?*, Bus. L. Today, November 2013, at 1 [hereinafter "Balough"] ("The potential exists that a car's computers, like any computer system, can be hacked, leaving the car vulnerable to infection by malware. These vulnerabilities pose serious safety hazards should they be exploited nefariously. Legal implications of this technological vulnerability have yet to be adequately addressed."). Cars contain dozens of Electronic Control Units (ECUs) "embedded in the body, doors, dash, roof, trunk, seats, wheels, navigation equipment, and entertainment systems," many of which connect to the internet and provide access points for hackers. *Id.* Disturbingly, "[t]he potential vulnerability of cars to hacking will increase as vehicle-to-vehicle (V2V) and self-driving cars become available" and "the average auto maker is about 20 years behind software companies in understanding how to prevent cyber attacks." *Id.* at 3.

24 Kelly Pleskot, *FCA Recalls 1.4 Million Vehicles Over Hacking Concern*, MotorTrend, Jul. 24, 2015, http://www.motortrend.com/news/fca-recalls-1-4-million-vehicles-over-hacking-concern/.

25 Craig Timberg, *Hacks on the Highway*, Washington Post, Jul. 22, 2015, at 3, http://www.washingtonpost.com/sf/business/2015/07/22/hacks-on-the-highway/ [hereinafter "Timberg"].

used-car dealership remotely accessed the company's computers and caused havoc by setting off car alarms and shutting down engines.[26]

The danger is not limited to cars. For example, in 2008, a fourteen-year-old boy hacked into the system controlling the trains of Lodz, Poland as a prank.[27] He made several trains change tracks, causing multiple derailments and injuries.[28] In 2013, the Federal Bureau of Investigation and the Department of Homeland Security "issued a warning" about "several... attacks against the 911 system."[29] The attacks were an attempt to extort money, and when the perpetrators received nothing they "launched [a] high volume of calls against the target network, tying up the system from receiving legitimate calls."[30] In 2016, Iranian hackers breached "the computer-guided controls" of the small Bowman Dam in suburban Rye Brook, New York.[31] The dam was offline for repair and immune to remote access, but the implications are disturbing because the hackers may have been trying to access an identically named dam in Oregon that is a formidable "245 feet tall and 800 feet long...."[32]

B. Other ways the IoT could be hacked

Security researchers have identified a range of other frightening vulnerabilities. Researchers have "demonstrated ransomware against home thermostats and exposed vulnerabilities in implanted medical devices.

---

26 *Id.* at 7; Matthew Shaer, *Disgruntled Hacker Remotely Disables 100 Cars*, Christian Science Monitor, Mar. 18, 2010, at 1, http://www.csmonitor.com/Technology/Horizons/2010/0318/Disgruntled-hacker-remotely-disables-100-cars.

27 Graeme Baker, *Schoolboy Hacks Into City's Tram System*, the Telegraph, Jan. 11, 2008 at http://www.telegraph.co.uk/news/worldnews/1575293/Schoolboy-hacks-into-citys-tram-system.html.

28 *Id.*

29 Kim Zetter, *How America's 911 Emergency Response System Can Be Hacked*, Washington Post: The Switch, Sep. 9, 2016 at 1, https://www.washingtonpost.com/news/the-switch/wp/2016/09/09/how-americas-911-emergency-response-system-can-be-hacked/?utm_term=.64b3faef0108.

30 *Id.* (internal citation omitted).

31 Joseph Berger, *A Dam, Small and Unsung, Is Caught Up in an Iranian Hacking Case*, N.Y. Times, Mar. 25, 2016, https://www.nytimes.com/2016/03/26/nyregion/rye-brook-dam-caught-in-computer-hacking-case.html?_r=0.

32 *Id.*

They've hacked voting machines and power plants."[33] Indeed, many computer security experts fear that the USB port on an airline seat could potentially control the airplane's avionics.[34]

Clearly, the IoT offers a broad array of dangerous tools for hackers can exploit for a range of motives, including: terrorism,[35] "national aggression,"[36] pranking,[37] election tampering,[38] and monetary extortion.[39] Whatever the impetus for hacking in the IoT, the threats moving forward are considerable.

II. Why is the IoT so insecure and vulnerable to hacking?

Security researches have attributed the scale and ease of attack to "the quantity of insecure IoT devices operated by a highly distributed set of unwitting consumers,[40] and to a "fundamental market failure."[41] Because electronics consumers care most about affordability, "the market has prior-

---

33 Schneier, *supra* note 2, at 5. at 5. Although there is evidence of Russian hacking intended to affect the U.S. presidential election in 2016, these efforts seem to have been focused on the computers themselves and information contained on them (e.g., emails and donor databases), rather than on things connected to the computers, such as voting machines. *But see* David Smith & John Swain, *Russian Agents Hacked US Voting System Manufacturer Before U.S. Election*, The Guardian, June 5, 2017, at 1 (noting that although hacking and release of Democratic emails had been traced to Russia vote counting "was thought to be unaffected" before leaked report that Russian intelligence hacked into U.S. manufacturer of voting systems weeks before election).

34 Schneier Testimony, *supra* note 5, at 102.

35 *See generally* Balough *supra* note 23, at 1 (theorizing about the possibility that cars might be exploited for terrorism through the internet).

36 Schneier Testimony, *supra* note 5, at 57.

37 *See* Baker, *supra* notes 27 & 28, and accompanying text (chronicling a hacking attack executed as a prank).

38 *See generally* Bruce Schneier, *American Elections Will Be Hacked*, N.Y. Times, Nov. 9, 2016, at https://www.nytimes.com/2016/11/09/opinion/american-elections-will-be-hacked.html (summarizing the vulnerabilities of voting machines and infrastructure and the danger of election fraud).

39 *See* Drew, *supra* note 22, at 3 ("The primary motivation for [DDoS] attacks appears to be financial.").

40 *See* Fu, *supra* note 8, at 4 ("What's new is the scale and ease of attack because of the quantity of insecure [IoT] devices operated by a highly distributed set of unwitting consumers.").

41 Schneier, *supra* note 2, at 3.

itized features and cost over security."[42] Thus, the teams that make many IoT devices have less "security expertise" than major companies like Apple, because "the market won't stand for the additional costs that [similar training] would require."[43] Further complicating matters, many IoT devices are part of a complex global supply chain where they are "designed and built offshore, then rebranded and resold."[44] The resulting devices are the product of differing international standards of security.[45]

As a result, IoT devices in the U.S. exhibit a wide range of serious vulnerabilities. Many come with "default and easily-identifiable passwords that hackers can exploit."[46] Some of these passwords cannot be changed.[47] Similarly, many "devices also lack the capability of updating their firmware, forcing consumers to monitor for and install updates themselves."[48] Additionally, consumers "often have little way to know when [IoT] devices have been compromised."[49] The relationship between hardware and software further exacerbates the problem. When the underlying software has been corrupted, the object it is connected to often continues to function as intended, leaving little reason to replace it.[50] Even devices used as part of a botnet in an attack will "still work fine."[51] Additionally, the hardware of an object may last far longer than the software that powers it remains secure.[52]

---

42 *Id.*
43 *Id.*
44 *Id.*
45 Dale Drew Committee on Energy and Commerce, *Understanding the Role of Connected Devices in Recent Cyber Attacks* (preliminary transcript), Hearing, pp 37–38 Nov 16, 2016. Available at: http://docs.house.gov/meetings/IF/IF17/20161116/105418/HHRG-114-IF17-Transcript-20161116.pdf; Accessed: 2/26/17 [hereinafter "Drew Testimony"] (explaining the need for international standards).
46 Drew, *supra* note 22, at 2.
47 *Id.*
48 *Id.*
49 *Id.*
50 See Fu Testimony, supra note 21, at 88 (using the example of an MRI machine to explain that consumers do not want to replace functioning hardware to fix a problem with vulnerable software, especially where the machine is expensive).
51 Schneier, *supra* note 2, at 4.
52 *Id.* at 3–4 (identifying the problem of longevity in internet enabled devices including cars, refrigerators, and thermostats).

III. The Internet of Things and the Current Legal Regime

This section explores the interaction between the IoT and the current legal regime. Subsection A discusses whether current laws prohibit hacking with an intent to control an object. Subsection B explores the problem of botnets. This section concludes that hacking in the IoT will often be illegal, though these laws punish conduct after the fact, but do not prevent it.

A. Scenario one: hacking with the intention of controlling an object

Consider the following hypothetical. Bill has a grudge against his neighbor Jeremy. He discovers that there is a security vulnerability in one of the many electronic control units (ECUs) of Jeremy's late model sedan,[53] and he hacks in through the internet and enters commands that take control of Jeremy's car.[54]

Bill's actions are increasingly plausible as cars become ever more connected and automakers struggle to update outmoded software.[55] The hypothetical identifies an intriguing problem in the IoT: the hackers' target is not the computer but rather the object it is connected to. This is true of many of the examples outlined above, although the motives varied: the fourteen-year-old hacked a train system for a prank; the Iranians hacked a dam possibly for terrorism; the extortionists attacked the 911 system for money; and the disgruntled employee hacked into cars sold by his former employer for revenge. All wanted to control an object, and the internet was just a means to that end.[56] In the IoT a key objective of remote access will be to control the "Things." Thus, a key question is whether the current

---

53 Such vulnerabilities are apparently not hard to track down. *See* Timberg, *supra* note 25.
("[S]ecurity researches" discovered "readily accessible Internet links to thousands of other privately owned Jeeps, Dodges and Chryslers....").

54 The exact form of hacking varies based on the specific ECU: "[s]ome entry points to a car's ECUs require a direct hard-wired connection, while others can be accessed wirelessly, including Wi-Fi or [Radio-frequency identification]." Balough *supra* note 23, at 1. Researchers demonstrated that once a vehicle has been started normally, key functions including the engine, brakes, and transmission can be controlled remotely by "typing on a MacBook Pro." Timberg, *supra* note 25.

55 Timberg, *supra* note 25.

56 *See supra* text accompanying notes 26–32.

legal regime covers this relatively new threat, and governs scenarios like the one with Bill and Jeremy. It does.

1. The Computer Fraud and Abuse Act

The most obvious law that could be employed to combat hacking with the intent to control is the Computer Fraud and Abuse Act ("CFAA"). The CFAA was "[o]riginally designed as a criminal statute aimed at deterring and punishing hackers, particularly those who attack computers used for compelling federal interests,"[57] but also includes "a trespass-like civil remedy under federal law" for various forms of hacking.[58] It is logical that the law would cover hacking with an intent to control an object, as it is believed that Congress passed the CFAA in response to the movie WarGames,[59] where the protagonist accidentally hacks into the computer controlling America's nuclear weaponry and nearly starts a third world war.[60]

Indeed, the provisions of the CFAA cover a range of conduct. The act prohibits:

> (1) unauthorized obtaining of national security information; (2) unauthorized obtaining of information from a financial institution, United States department or agency, or from any protected computer; (3) unauthorized access to government computers; (4) computer fraud; (5) computer damage; (6) passwords trafficking; and (7) computer extortion.[61]

---

57 COMPUTER FRAUD AND ABUSE ACT, SS032 ALI-ABA 993, 995.

58 5.06. Computer Fraud and Abuse Act, 1 E-Commerce and Internet Law 5.06 (2016 update).

59 *See* Fred Kaplan, *'War Games' and Cybersecurity's Debt to a Hollywood Hack*, N.Y. Times, Mar. 25, 2016, at https://www.nytimes.com/2016/02/21/movies/wargames-and-cybersecuritys-debt-to-a-hollywood-hack.html?_r=0 (chronicling the emergence of early federal cybersecurity laws in response to President Ronald Reagan's concern over the movie "WarGames"); Jay P. Kesan & Carol M. Hayes, *Mitigative Counterstriking: Self-Defense and Deterrence in Cyberspace*, 25 Harv. J.L. & Tech. 429, 492 (2012) [hereinafter "Kesan"].

60 For a synopsis of the movie Warm Games, see http://www.imdb.com/title/tt0086567/synopsis?ref_=tt_stry_pl (last visited August 31, 2017).

61 Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, 14 U. Pitt. J. Tech. L. Pol'y 158, 163 (2014) [hereinafter "Vasiu"].

Section 1030(a)(5) is the subsection most likely to cover hacking with an intent to control an object. It criminalizes:

> knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer; intentionally access[ing] a protected computer without authorization, and as a result of such conduct, recklessly caus[ing] damage; or intentionally access[ing] a protected computer without authorization, and as a result of such conduct, caus[ing] damage and loss.[62]

Whether § 1030(a)(5) prohibits hacking with an intent to control hinges on four key definitions: (1) "transmission," (2) "computer," (3) "protected computer," and (4) "damage."

"Transmission" encompasses a range of hacking activities, such as "[t]he transfer of operation or confidential information," "malicious software updates," "code injection attacks," DDoS, and the "embedding of malicious code" or malware.[63] Under the CFAA, transmission "can be accomplished either over the Internet or through a physical medium such as a compact disc."[64] This would cover many forms of hacking aimed at controlling an object. To return to the example of Bill and Jeremy, Bill's conduct qualifies, as he transmitted commands via the internet to take control of Jeremy's car.

Within the CFAA, "computer" is an expansive term. It defines a computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device...."[65] As Judge Easterbrook explained, the definition of "computer" in the CFAA is an example where the exclusions from the definition "show just *how* general" it is."[66] Indeed, CFAA subsection (e)(1) "carves out automatic typewriters, typesetters, and handheld calculators; this shows that other devices with embedded processors and software are covered."[67] Thus, most IoT devices are computers. The ECUs that Bill hacked in Jeremy's car cer-

---

62 18 U.S.C. § 1030(a)(5) (2012).
63 Vasiu, *supra* note 61, at 167–169.
64 174 A.L.R. Fed. 101 (Originally published in 2001).
65 18 U.S.C. § 1030 (e)(1) (2012).
66 *United States v. Mitra*, 405 F.3 d 492, 495 (7th Cir. 2005).
67 *Id.*

tainly would qualify, as they "are high speed data processing devices performing logical, arithmetic, or storage functions."[68]

Many IoT devices will also be *protected* computers. The CFAA defines protected computers to include not only those "exclusively for the use of a financial institution or the United States Government" but also computers "used in or affecting interstate or foreign commerce or communication...."[69] Courts have interpreted this definition broadly. Indeed, in *U.S. v. Mitra*, Judge Easterbrook explained that "the statute... protects computers (and computerized communication systems) used in such commerce, no matter how the harm is inflicted. Once the *computer* is used in interstate commerce, Congress has the power to protect it from a local hammer blow, or from a local data packet that sends it haywire."[70] This standard included the afflicted computer in *Mitra*—Madison, Wisconsin's "computer-based radio system for police, fire, ambulance, and other emergency communications"[71]—even though the hacker's "interference did not affect any radio system on the other side of a state line."[72] What mattered was that Madison's computerized radio system "operated on spectrum licensed by the FCC" and therefore implicated interstate commerce.[73]

Mitra is not an exception. Particularly relevant for devices that are part of the *IoT*, "[c]ourts generally hold that because the Internet and interstate commerce are inexorably intertwined, any computer connected to the Internet should be considered a computer affecting interstate commerce and therefore protected."[74] Thus, if Jeremy's ECU is internet-enabled, it is a protected computer under the CFAA. This seems a safe bet in an era where cars are increasingly connected and can "talk to the outside world through remote key systems, satellite radios, telematic control units, Bluetooth connections, dashboard Internet links and even wireless tire-pressure monitors."[75]

---

68 Balough *supra* note 23, at 3.
69 18 U.S.C. § 1030 (e)(2)(b)(2012).
70 *Mitra*, 405 F.3 d at 496.
71 *Id.* at 493.
72 *Id.* at 496.
73 *Id.*
74 Vasiu, *supra* note 61, at 164.
75 Timberg, *supra* note 25.

"Damage" is "defined as 'any impairment to the integrity or availability of data, a program, a system, or information,'"[76] and almost certainly encompasses hacking with the intent of controlling an object.[77] To begin with, a hacker damages a computer under the statute by forcing it to behave in a manner unintended by its owner.[78] Additionally, "[a]dverse actions.... that alter, encrypt, encipher, encode, transmit or delete data or exhaust system resources" all are damage under the CFAA because they impair the availability of the computer by making it unusable and inaccessible.[79] Transmission is damage under the CFAA because it "involves the deletion of computer data or files."[80] Clearly, Bill damaged Jeremy's car under the CFAA, since he caused it to behave contrary to the wishes of its owner.

Finally, CFAA penalties are structured in a manner that enhances punishment depending on the outcome of the hacking. The Act provides harsher penalties for those whose hacking causes "physical injury," "a threat to public health or safety," "damage affecting a computer used by or for an entity of the United States government in furtherance of justice, national defense, or national security," damage to at least ten computers within a year, or "modification or impairment... of the medical examination, diagnosis, treatment, or care of 1 or more individuals...."[81] Unsurprisingly, the stiffest retribution is reserved for those who "knowingly or recklessly caus[e] death from conduct in violation of" subsection (a)(5)(a).[82] Depending on the nature and results of Bill's hacking, he may be subject to some of these increased CFAA penalties. For example, if he took control of Jeremy's car while it was hurtling down a busy highway, it is easy

---

76 Jeffrey K. Gurney, *Driving into the Unknown: Examining the Crossroads of Criminal Law and Autonomous Vehicles*, 5 Wake Forest J.L. & Pol'y 393, 439 (2015) quoting 18 U.S.C. § 1030(e)(8) (2012)) [hereinafter "Gurney"].

77 As one commentator has summarized it, "nearly any instance of unauthorized hacking could be said to impair the integrity of a computer system." Ric Simmons, *The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime*, 84 Geo. Wash. L. Rev. 1703, 1712 (2016).

78 *See* Vasiu, *supra* note 61, at 160 ("Integrity generally refers to maintaining computer data in a protected state, unaltered by improper, unauthorized or subversive conduct or acts contrary to what the system owner or privilege grantor intended.").

79 *Id.*

80 *Id*. at 192.

81 18 U.S.C. § 1030(c)(4) (2012).

82 18 U.S.C. § 1030(c)(4)(F) (2012).

to imagine how Bill might have threatened public safety. If Jeremy's car crashed as a result of the hacking, Bill would face steeper sentencing under the CFAA if Jeremy was injured or killed.

2. Other laws

There are many other laws that could govern hacking with an intent to control an object. Although a full review is beyond the scope of this paper, this subsection summarizes a few obvious candidates.

One way to punish hacking with an intent to control an object is to look to state versions of the CFAA. All "fifty states... enact[ed] statutes specifically prohibiting computer misuse."[83] Like the CFAA, all of these laws employ the "common building block of unauthorized access to a computer," which is "usually supplemented by other elements to create additional criminal prohibitions, such as statutes preventing... computer damage."[84] Many of these laws could be construed as anti-hacking statutes.[85] Such laws could provide a useful tool in combatting hacking in the IoT. For example, Connecticut General Statute § 53-451(b) makes it "unlawful for any person to use a computer or computer network without authority and with the intent to... (2) Cause a computer to malfunction, regardless of how long the malfunction persists." Given the statute's broad definition of computer,[86] it would almost certainly govern hacking in an attempt to control an object. Other states have similar laws.[87] If the hypothetical involv-

---

83 Computer Crime Law, 29.

84 *Id*. at 29–30.

85 Gurney, *supra* note 76, at 434.

86 *See* Conn. Gen. Stat. § Sec. 53-451(a)(1) (2015) ("'Computer' means an electronic, magnetic or optical device or group of devices that, pursuant to a computer program, human instruction or permanent instructions contained in the device or group of devices, can automatically perform computer operations with or on computer data and can communicate the results to another computer or to a person. 'Computer' includes any connected or directly related device, equipment or facility that enables the computer to store, retrieve or communicate computer programs, computer data or the results of computer operations to or from a person, another computer or another device.").

87 *See* Gurney, *supra* note 76, at 436 ("States also have vandalism hacking statutes. Unlike the trespassing statutes, the vandalism statutes "typically make it a more serious crime to purposely access a computer without authorization and alter, damage or disrupt the operation of the computer and/or the data it contains.").

ing Bill and Jeremy occurred in a state like Connecticut, than Bill would have violated state law by causing the ECU in Jeremy's car to behave in a manner other than its intended use.

Additionally, other state computer crime provisions may cover hacking in the IoT, depending on the outcome of the conduct. Indeed, several states "make it an offense to break into or tamper with a computer system and thereby cause the death of one or more persons or create a strong probability of causing death to one or more persons."[88] Relatedly, some state computer crime laws prohibit damaging the object for which control is sought, or other property.[89] Thus, if Bill damaged Jeremy's car, or Jeremy himself, he is likely culpable under additional state computer crime laws.

Of course, depending on the results of, and motivations behind, hacking, other non-computer crime laws might apply as well. For example, Bill might be culpable for kidnapping, joyriding, grand larceny, or even "[d]estruction of motor vehicles or motor vehicle facilities" under 18 U.S.C. § 33(a) (2012).[90] If Bill intends to kill Jeremy, and succeeds, he might be liable for murder.[91] In the IoT, hacking will often be a method for perpetrating another crime: as a result, other statutes will likely apply.

B. Scenario two: botnets

As discussed in Section I, botnets are a network of compromised computers, "often programmed to complete a set of repetitive tasks" without "the owner's knowledge or permission."[92] Botnets "are the instrumentality through which substantial amounts of cybercrime takes place."[93] Botnet based cybercrime includes spam, fraud, and—of particular relevance for the IoT—DDoS and the installation of malware.[94] Hackers used a botnet

88 Susan W. Brenner, *State Cybercrime Legislation in the United States of America: A Survey*, 7 Rich. J.L. & Tech. 28, 10 (2001).

89 See, e.g., Conn. Gen. Stat. § 53-451 (b)(5) (criminalizing "use [of] a computer or computer network without authority... with the intent to: Cause physical injury to the property of another....").

90 Gurney, supra note 76, at 433–442.

91 *Id*. at 438.

92 Lerner, *supra* note 13, at 237–38 (2014).

93 Zachary K. Goldman & Damon McCoy, *Deterring Financially Motivated Cybercrime*, 8 J. Nat'l Security L. & Pol'y 595, 608 (2016) [hereinafter "Goldman"].

94 Lerner, *supra* note 13, at 237–38.

in the Dyn attack, which prompted the HECC hearing discussed in Section I, about the dangers of hacking in the IoT.[95]

Unsurprisingly given the nature of their use, botnets are illegal under the CFAA.[96] For example, CFAA section 1030(a)(5) criminalizes "knowingly caus[ing] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally caus[ing] damage without authorization, to a protected computer...."[97] Botnets are often created through malicious software that behaves in this manner.[98] Although there are practical problems to combating Botnets with laws like the CFAA,[99] there have been successful prosecutions.[100]

IV. Improving the Security of the IoT

Although the CFAA provides a tool to prosecute hacking in the IoT, the dangers in this new era are numerous and grave. As a result, better security in the IoT also requires a reduction of vulnerabilities and a mechanism for prevention.

As section II illustrates, the IoT is currently the victim of a market failure.[101] Consumers want IoT devices to be as cheap as possible.[102] Manufacturers and retailers oblige, prioritizing cost over security because they

---

95 *See* text accompanying notes 10–22 *supra*; Bruce Schneier, *Lessons From the Dyn DDoS Attack*, Schneier on Security (November 8, 2016, 6:25 AM), https://www.schneier.com/blog/archives/2016/11/lessons_from_th_5.html.

96 *See* Kesan *supra* note 59 at 493 ("The CFAA's language is very broad and can be read to prohibit the creation of botnets.").

97 18 U.S.C. § 1030(a)(5) (2012).

98 *See* Kesan *supra* note 59 at 442–444 (explaining how botnets are created).

99 *See* Lerner, *supra* note 13, at 244 ("CFAA enforcement requires precise knowledge of the defendant's identity, which is often impossible to obtain in DDoS attacks... [In addition] CFAA prosecution of DDoS masters in foreign countries is impeded by a number of jurisdictional obstacles.").

100 *See*, e.g. Department of Justice Office of Public Affairs, *Arizona Man Sentenced to 30 Months in Prison for Selling Access to Botnets*, Justice News (September 15, 2014), https://www.justice.gov/opa/pr/arizona-man-sentenced-30-months-prison-selling-access-botnets (describing successful prosecution of a man who had sold "access to and use of thousands of malware-infected computers").

101 *See* text accompanying note 41, *supra*.

102 *See* text accompanying note 43, *supra*.

have no incentive not to.[103] International supply chains and the limited security expertise of many IoT design teams further complicate matters.[104] The widespread weaknesses in IoT devices offer an enticing tool and opportunity for nefarious activity. As a result, the IoT of today is a veritable wild west of the digital era, where a new frontier invites violence, theft, and mischief. To continue the metaphor, if existing laws are insufficient to remedy the dangers of the IoT, what *will* tame the west?

There are many possibilities,[105] and this section explores two options: a standards based approach, and a new or expanded regulatory agency. A third intriguing approach, sketched briefly below, is counter hacking.

A. The Standards Approach

Vulnerabilities like default passwords and static firmware threaten IoT security. Although devices with these vulnerabilities are suboptimal, they are not technically substandard. There is no uniform set of standards that IoT manufacturers or retailers must meet.[106] The standards approach would attempt to remedy this by imposing such a system on key players.

A standards system would combat the market failure by incentivizing better security practices in the proliferation of IoT devices.[107] According to one expert, adopting "defined standards" will "change buying and investment patterns" that are responsible for the current state of vulnerability in the IoT.[108] Imposing stronger security measures through standards for IoT developers is important because "[s]ecurity needs to be built into IoT devices, not bolted on. If cybersecurity is not part of the early design of an

---

103 *Id.*

104 *See* text accompanying note 44–45, *supra*.

105 *See, e.g.,* IoT Security Foundation, *IoT is Vast and Has Many Security Related Issues – how do we go about addressing them?*, IoT Security Foundation, https://iotsecurityfoundation.org/working-groups/(last visited Nov. 14, 2017) (listing and summarizing different practice groups, each focused on a different aspect of IoT security).

106 *See* Drew, *supra* note 22, at 4 ("The current lack of any security standards for [IoT] devices is certainly part of the problem that ought to be addressed.").

107 *See Id.* ("IoT manufacturers and vendors should embrace and abide by additional security practices to prevent harm to users and the internet.").

108 *See* Drew Testimony, *supra* note 45, at 97.

IoT device, it's too late for effective risk control."[109] Establishing standards that require better security measures from the start implicates "domestic and international" standards setting entities like the International Standards Organization or the National Institute of Standards and Technology (NIST),[110] and may require government intervention.[111]

Generally, organizations advocating for the use of a standards-based approach emphasize the importance of a consistent and uniform standard,[112] but the priorities of an IoT security standard might vary. For example, Dale Drew—a proponent of a standards approach—is preoccupied with remedying vulnerabilities like default passwords, "hard-coded credentials," and the "lack of capability of updating [IoT device] firmware."[113]

Assuming arguendo that agreement could be reached on the correct standards, this approach would still have a serious limitation: it would not affect the millions of existing devices.

B. Agency Regulation

Some experts have concluded that the pervasive threats to the IoT, and the related market failure, require increased government involvement.[114] They argue that "[c]ybersecurity ought to be a public good much like automo-

---

109 Fu, *supra* note 8, at 3.

110 *See* Drew Testimony, *supra* note 45, at 97–8. Indeed, the Institute of Electrical and Electronics Engineers is currently working on "P2413," a "standard for an architectural framework for the [IoT]" which will address security among other considerations. IEEE Standards Association, *Standard for an Architectural Framework for the Internet of Things (IoT)* IEEE (2017), http://grouper.ieee.org/groups/2413/.

111 *See* Drew, *supra* note 22, at 4 (Noting that in the context of standards setting, "there may be a role for the government to provide appropriate guidance").

112 *See Standard for an Architectural Framework for the Internet of Things*, IEEE Standards Association (2017), https://standards.ieee.org/develop/project/2413.html ("The adoption of a unified approach to the development of IoT systems will reduce industry fragmentation and create a critical mass of multi-stakeholder activities around the world.").

113 Drew, *supra* note 22, at 2.

114 *See* Schneier Testimony, *supra* note 5, at 43 ("The choice is not between government involvement and no government involvement, but between smart government involvement and stupid government involvement.").

bile safety."[115] One possible option to achieve that goal is to expand the capabilities of existing government agencies to test IoT security. To promote automobile safety, there are federally funded research and development centers, testing facilities run by the National Transportation Safety Board (post market), automotive crash safety testing (premarket), and the Nevada National Security Site (destruction and survivability testing). [116] But no analogous regulatory or research entities exist to provide a proving ground for the types of embedded cybersecurity defenses needed to guard the IoT.[117] Such a facility would remedy the government's lack of a means to "conduct thorough security testing and assessment on IoT devices" and would reduce the inefficiencies of having diffuse entities conducting independent research.[118] This expansion could potentially fall under the control of the National Science Foundation or the NIST.[119]

Another possibility is the creation of a new regulatory agency. Schneier advocates for this position and analogizes the IoT to the technologies of the past that gave rise to new agencies: "trains, cars, airplanes, radio, and nuclear power."[120] He argues that "[i]n the world of dangerous things, we constrain innovation,"[121] and that the IoT presents new dangers just as those technologies did during their development. As a result, even if regulation would stifle some creativity, Schneier suggests that this is a necessary sacrifice for security.[122] Furthermore, the IoT presents problems that the market cannot or will not solve on its own. The most prominent is the market failure and the lack of consumer and manufacturer incentives to resolve technological vulnerabilities in the IoT.[123] Schneier argues that as with environmental pollution, regulation is essential because the dangers and ill effects occur downstream.[124]

---

115 Fu, *supra* note 8, at 8.
116 *Id.* at 3.
117 *Id*.
118 *Id.* at 8–9.
119 See Fu Testimony, *supra* note 21, at 35 (advocating for increased support for these agencies).
120 *See* Schneier Testimony, *supra* note 5, at 31.
121 *Id.* at 59.
122 *See* Id. ("So, yes, this is going to constrain innovation... but this is what we do when innovation can cause catastrophic risk.").
123 *Id.* at 58.
124 *Id.*

In the current political environment, which favors smaller government and reducing regulation, it seems doubtful that this approach could get traction in Congress. And if it did so, recruiting the necessary expertise and resources could be a daunting task.

C. Legalizing Strikebacks

The far more difficult question is what measures can be taken legally to eliminate the threat posed by botnets. This is a pressing consideration because without curative solutions, botnets can be used in multiple crimes.[125] Once a device is recruited into a botnet, it becomes part of a "commodity" that can be rented out "by the hour" or purchased.[126] Relying on enforcement and litigation does little to prevent future attacks, and "is inherently *ex post facto*."[127]

Remedial actions, sometimes referred to as counterstrikes or hack backs,[128] could provide a solution to the botnet problem. These actions might "enable attacked parties to detect, trace, and then actively respond to a threat by, for example, interrupting an attack in progress to mitigate damage to the system."[129] Specific strategies could include implementing a "DoS attack at the botnet controller or hacking the botnet controller and thereby taking control of the botnet."[130] However, not all remedial efforts are so forceful: "Hacking back against a botnet can be as simple and nonaggressive as pushing security patches onto infected computers, just as patients with a deadly virus could be forcibly treated or quarantined to prevent a contagion's spread."[131] Either way, these methods have the potential to help combat botnets and prevent future attacks.

---

125 One illustration of the resilience of botnets can be found in Microsoft and Europol's attempt to dismantle the ZeroAccess botnet: though portions of the botnet were taken down, it was revived within months. Goldman, *supra* note 93, at 610.

126 Janine S. Hiller, *Civil Cyberconflict: Microsoft, Cybercrime, and Botnets*, 31 Santa Clara High Tech. L.J. 163, 168–69 (2015).

127 *See* Kesan, *supra* note 59, at 474.

128 *See* Kesan, *supra* note 59, at 434 (using the terms "hack back" and "counterstrike").

129 *Id.* at 475.

130 *Id.*

131 Patrick Lin, *Ethics of Hacking Back*, U.S. Nat'l Sci. Found. (Sept. 26, 2016), http://ethics.calpoly.edu/hackingback.pdf.

The problem is that such behaviors may be illegal.[132] Ironically, "[t]he same laws that make it illegal to hack in the first place—for instance, to access someone else's system without authorization—presumably make it illegal to hack back."[133] The CFAA both criminalizes botnets and limits recourse against them.[134] The Department of Justice, the FBI, and "White House officials" have all suggested that such remedial efforts may be illegal.[135]

As a result, the legal regime that is intended to protect the public from hacking also limits the extent to which such dangers may be fought. Could counter hacking be legalized? It would raise a host of issues. For example, what would be sufficient to trigger the authority to hack back? Would advance authorization be required? What safeguards would be necessary? Note that botnets may infect millions of computers. What mechanism or procedures could be devised to ensure that the parties who wished to hack back would not do more harm than good? Even if counter hacking is justified in a given instance, what about the danger of misattribution and the potential for injury to innocent parties? From an ethical standpoint, does counter hacking invite vigilantism? Questions abound, and the answers are not easy.

V. Conclusion

The extraordinary growth of the IoT and its extreme vulnerability threaten individuals, businesses, and the broader society. In the United States, federal and state law include offenses that criminalize a wide range of conduct involving the misuse of the IoT. But even the successful prosecution of those offenses—when the offenders can be identified and the U.S. has jurisdiction—does nothing to address two fundamental problems: the enormous number of insecure devices already in use, and the fundamental market failure that continues to bring insecure devices onto the market. The situation is urgent, and policymakers must find new approaches to address these structural problems.

---

132 *See* Kesan, *supra* note 59, at 475 ("Even though counterstrikes are currently of questionable legality....").
133 Lin, *supra* note 131 at 6.
134 *Id.* (Identifying CFAA as a law contributing to this paradox).
135 *Id.*

Robotics and Criminal Law. Negligence, Diffusion of Liability and Electronic Personhood

*Susanne Beck**

"Robot kills worker at Volkswagen plant in Germany"[1] – even the Guardian and other foreign newspapers have reported on this tragic incident which took place two years ago. And although in this case the robot was a traditional one and the incident probably was caused by human error instead of malfunctioning of the machine, it has to be taken into account that such tragic accidents will contribute to the debate about interactions between robots and humans and the legal consequences of damages caused by machines. The phrasing itself is interesting: While in other contexts one would refer to an accident, here most papers talk about the robot as an active participant who "killed" the worker. This indicates an active role of the machine, a different perception of the inclusion of robots, a new fear of society.

Similarly, there has been a vivid discussion after a fatal accident of a Tesla self-driving car.[2] The unpredictability of the car was reflected as threatening and the debate was slowed down mainly by the realisation that the driver has been inattentive and not followed the instructions given by Tesla. Therefore, Tesla's self-driving system was cleared by federal auto-safety regulators.[3] As the autopilot required the driver's attention at all times, the driver was regarded as liable for the accident. But still, the debate showed the existing scepticism towards this new technology.

Therefore, it is important to discuss the legal situation right now, before even more major incidents influence the public debate in a negative way

---

* Prof. Dr. iur. Susanne Beck, LL.M. (LSE), Leibniz Universität Hannover.

1 http://www.theguardian.com/world/2015/jul/02/robot-kills-worker-at-volkswagen-plant-in-germany.

2 https://www.nytimes.com/2016/07/02/business/a-fatality-forces-tesla-to-confront-its-limits.html?action=click&contentCollection=Business%20Day&module=RelatedCoverage&region=EndOfArticle&pgtype=article.

3 https://www.nytimes.com/2017/01/19/business/tesla-model-s-autopilot-fatal-crash.html.

and hinder the technology unnecessarily. It also is crucial to determine the individual risks of the persons involved to be legally liable, because this might be another hindrance – if the risk of personal liability is too high it might to lead to the technology not being developed at all or at least not in a riskful way. New technological developments often challenge society and its normative framework, thus, regulations have to be created to deal with new dangers such as robotics – and it is important to create these laws as soon as possible.[4] But also, the existing laws have to be applied in a way that reflects the special dangers as well as advantages of these new technologies.

1. The Current Development of Robotics from a Legal Perspective

Robots will, in the years to come, play a more important role in many areas of life. They will work with us, support us when we are sick or immobile, drive us independently and maybe even educate our children, entertain us when we are lonely, give us advice when we are helpless. For performing these tasks, the machines have to become more and more „autonomous"[5] because it is not possible to give detailed orders for all relevant situations beforehand. Therefore one has to create machines which are able to learn, to adapt (e.g. to the communication style of its user, to his eating habits, to his body functions) and to be trained to react in the best suited way for the user. It is quite possible that for some of these tasks, especially when speed is crucial, the decision of a machine might be quicker, more rational, more informed than a human decision.[6] In general, machines will decide differently to humans – differently does not neces-

4 For specific regulation issues of robotics, see RoboLaw Group, Guidelines on Regulating Robotics: http://www.robolaw.eu/, 2014; see also Leroux et al., Suggestions for a Green Paper on Legal Issues in Robotics, 2012 and the suggestions of the Legal Affairs Committee of the European Parliament, http://www.europarl.europa.eu/news/en/press-room/20170110IPR57613/robots-legal-affairs-committee-calls-for-eu-wide-rules.

5 "Autonomous" is used in a broad sense here, meaning a certain space for decision-making for the machine. For a project working on different understandings of autonomy see http://www.isi.fraunhofer.de/isi-de/v/projekte/WAK-MTI.php.

6 Arkin, Governing Lethal Behavior: Embedding Ethics in a Hybrid Deliberative / Reactive Robot Architecture, GIT-GVU-07-11, 2008, p. 2, https://smartech.gatech.edu/jspui/bitstream/1853/22715/1/formalizationv 35.pdf.

sarily mean better or worse, though. In all probability, their decisions will be oriented on rationality and efficiency and less on empathy or emotionality, but, as mentioned, for some tasks this actually might be valuable.

One relevant feature of these new kinds of machines is that when programming the machine one cannot predict how it will act in a specific situation. It will become almost impossible to reconstruct ex post why the machine reacted in a specific way.

The common denominator of these kinds of machines is that their function is to disburden humans of making decisions of one kind or another. Humans might only decide beforehand where and when to use autonomous machines and give them guidelines but leave the assessment of the situation to the machines, sometimes even with the ability to learn from former experiences to advance their decision making process. That such developments carry risks and side effects and mistakes in the decision-making-process leading to damages cannot be doubted. As already mentioned, machines will decide differently, and therefore it is even thinkable that machines make „right" – from the perspective of the machine – but morally questionable decisions. One could even fear the dehumanisation of society in different social concepts when machines take over more and more of our human tasks.

Because of this, it often is postulated that there always, or at least in some contexts, should be a "human in the loop" of the decision making process. Thus, the decision would still be based on human morals, empathy, and potential liability of the human involved. One has to realise, though, that in many situations, this might lead to excessive demand and responsibility of the human in question. The driver of an autonomous vehicle, for example, does need at least 6 seconds to overtake – too long for most traffic situations. In other contexts, the mental influence of the suggestions by the machines is high as well, thus the decision by the human in the loop is determined in a way that might lead to doubts about his responsibility. At least, one should be aware that even when there is a human in the loop one cannot speak of a human decision anymore, but a decision made by human and machine collaboratively.

2. Legal Questions – Overview

The deployment of autonomous machines will lead to questions in different legal areas. The functioning of autonomous machines will require col-

lecting and processing enormous amounts of data – of course, this could collide with the existing data protection regime.[7] There will be questions not just about the intellectual property rights of programmer, producer and user but also about these rights if the robot produces something by itself. It will have to be discussed – in labour law – if one can be forced to co-work with robots. In international law, one is debating about the legality of Autonomous Weapon Systems.

In the following, I want to focus on the law dealing with the risks of robots instead of the just mentioned, very specific legal questions. Risks can be dealt with in public law (here one can discuss the conditions for usage of these machines and the areas of life in which they can be used), in civil law and in criminal law. Concerning legal handling of risks, the debate resembles other debates in which modern risks are analysed from a legal perspective, e.g. the Internet, Biotechnology, the importance of cooperation and thus the responsibility diffusion in collectives. All this can be summarised as „Risk Society" – and how this kind of society can be regulated, controlled or governed has been discussed over the last decades.

Adapting the legal system to the development in robotics can mean to enact laws in the area of public law, civil law and criminal law, to interpret existing laws in a specific way, to take non-state regulations into account.

2.1. Public Law: Controlling the Risks

In Public Law one discusses, inter alia, if the administrative laws in certain areas have to be adapted to the usage of autonomous machines – be it the laws about medical devices, the traffic laws, laws about the conduct of research in private or public areas, etc. Additionally, the security standards are introduced by non-governmental institutions such as International Organization for Standardization (ISO). The interaction of state and social norms, of government and governance, is challenged by the development of robotics, because no social standards for adequate behaviour exist until now and one is challenged by having to develop such standards from scratch. While in other areas standards such as ISO-norms are generally well integrated into the legal system (with exceptions, of course), this is

7 Leroux et al., Suggestions for a Green Paper on Legal Issues in Robotics, 2012, pp. 46 et seqq.

sometimes questioned in the area of robotics – it seems to be an area in which the intransparency of these standardizations has become more obvious and problematic, maybe because of the new developments, the missing discussion in society, the impossibility of orientating the standards to other areas of life. Later on, we will come back to the debate that circles around how to develop socially acceptable security standards for such an important, dangerous and unpredictable new technology as the development of "autonomous" machines.

Additionally, robots can be used as assistance against risks, be it in natural disasters, in war or as assistants of police and security organisations. Here one will have to discuss in future in which cases it is proportional to use until now unpredictable and maybe not fully controllable machines. In general: As far as autonomous machines are probably faster and can guarantee better risk management than human assistants, and as far as in these cases one can avoid risking the lives of human helpers, it is more than plausible to use machines.

2.2. Civil Law: Liability for Damages

In Civil Law it is, for example, questionable who is liable for contracts closed by autonomous machines or for damages caused by these machines. Differently to traditional machines, it is not plausible to regard electronic agents as mere tool of the user – the decision making range of these machines is too broad for such a categorisation. The existing regimes of liability for damages are also not applicable, at least not without adaptation. With

One also needs to discuss how to deal with the necessary insurances, if it might, e.g., be possible to force insurances to contract with the users of such machines, which categories they belong to, if these machines can only be used if insured, etc.

With regard for some of these problems it also is debated if and how electronic agents can interact as legal actors.[8] A new legal actor[9] might be necessary because the traditional liability concepts (e.g. negligence, prod-

8 Hanisch, Haftung für Automation, 2010.

9 Leroux et al., Suggestions for a Green Paper on Legal Issues in Robotics, 2012, pp. 58 et seqq.

uct liability or strict liability) are difficult to apply in the context of autonomous machines.[10]

2.3. Criminal Law: Responsibility for the Robot`s Action?

Robots will participate in traffic and be used as tools, and in all these contexts it is possible that they will be used to commit crimes – this will lead to specific debates if the action in question fulfils a specific criminal law (traffic laws, trespass, etc.).

But more relevant in criminal law will be the question of criminal responsibility for the robot's damaging a third party. Criminal Law generally is based on the damnable conduct of the offender, on his intent or negligence about the violation of the goods of a third party. All this is challenged by the usage of "autonomous" machines. Even if we are talking merely (for the moment) about machines acting in a dynamic and unstructured environment based on feedback information[11], it is almost impossible to pinpoint one individual which is criminally responsible if the machine has violated the rights / goods of a third party.[12]

3. Focus: Robotics and Criminal Law

Public law mainly addresses the conditions to balance the interests of the individuals involved or potentially restricted or violated by this new technology, and civil law mainly discusses the contracts and the financial balancing in case of damages. In these areas of law, the main threat for the people developing and producing robots is to be financially liable, a threat that can be dealt with beforehand, by insurance or by collective payments of the parties involved in the development of the technology, for example.

---

10 Beck, Dealing with the diffusion of legal responsibility: the case of robotics, in: Nida-Rümelin / Bisol (eds.), Technical Options and Ethical-Legal Responsibility, 2014, pp. 167 et seqq.

11 Jain, Autonomous weapon systems: new frameworks for individual responsibility, in: Bhuta et al. (eds.), Autonomous Weapons Systems – Law, Ethics, Policy, 2016, pp. 303 et seqq.

12 ibid.

It is differently in the context of criminal law: Here it is not possible to avoid individual responsibility, on the contrary: Each party is responsible for its own actions.

Several individuals could be considered as perpetrator: the producer, the programmer, the seller or the user of the robot. In most cases the humans involved will not have intent about the specific action of the machine. Still, the violation of another human being could lead to criminal liability arising from negligence. This kind of criminal liability can be connected to every stage of the production process and usage, including research and development.

The first requirement of negligence is that the person whose liability is discussed acted without "reasonable care"[13]. The standard of care is usually determined by a person's expected form of behaviour in a given situation. As indicators one can refer to non-legal standards, such as ISO and DIN standards.[14] As we have already heard, developing these standards is difficult in the area of robotics. When determining the standard of care for people involved in research and production of robots, there are especially two important things to note:

First of all, at the moment, only few standards exist for the here relevant areas of robotics.[15] One reason for the slow development of standards is that the machines these standards would be relevant to are still in development and the knowledge about possible risks (kind and intensity) is still low. Standardising institutions are challenged not just by determining how to avoid inadequate risks but also by deciding which risks actually are inadequate. In such cases, the general-social standard of rationality is applied additionally: How would a rational person have acted to avoid damage in a similar situation? This vague evaluation, though, offers only little help in complex technological fields such as robotics.[16]

Secondly, non-legal norms only are indicators for whether the actions of a person were consistent with the legal standard of care. They also are, generally, developed with regard to civil liability instead of criminal law. Criminal law is not simply an accessory to the regulations of non-govern-

---

13 Kudlich in: Heintschel-Heinegg B (ed.), Beck-OK StGB, § 15 para 35 et seqq.

14 See, e.g., BGHSt 4, 182 (185); sceptical: Duttge, in: Joecks / Miebach (eds.) Münchener Kommentar StGB, § 15 para 114 et seqq.

15 See, e.g.: ISO 10218-1: 2006; ISO 8737: 2011; ISO 10218-2: 2011; ISO 13482: 2014.

16 Duttge, in: Joecks / Miebach (eds.) Münchener Kommentar StGB, § 15 para 114.

mental groups, thus one must always additionally consider overall social morality[17]. If certain internal rules do not contradict social expectations and standards of rationality, and if any party in question has recognized this deficiency, liability for negligence must be included in the determination of criminal liability.

For considerations on the few already existing standards in robotics as well as on the process of developing such standards it is necessary to consider the two relevant perspectives: The perspective of standardising institutions can probably best be shown by quoting the German DIN-Institute itself (my own translation): "Standards foster global trade and serve rationalisation, securing of quality, protection of society as well as safety and communication. Economic growth is influenced stronger by standards than by patents or licences. Standards are strategic instruments in competition."[18] Even if the protection of society is mentioned, it becomes clear that the standardising actors are also aiming for economic advantages.[19]

This has to be contrasted with the perspective of criminal law: Criminal law does not only serve to minimise risks and prevent danger. It also stabilises the normative consciousness of society concerning actions that are regarded as socially inadequate. Thus the danger of a certain action is not sufficient to penalise it; it also is necessary that it violates social-moral rules[20]. These rules have to be – in theory – accepted by every member of society, which could be an indicator for specific norms based on singular interests (of specific groups) not fitting the criteria for enacting criminal laws. One has to be aware, though, that society accepts – and actually

17 Lackner / Kühl StGB, § 15 para 39.

18 „Normen fördern den weltweiten Handel und dienen der Rationalisierung, der Qualitätssicherung, dem Schutz der Gesellschaft sowie der Sicherheit und Verständigung. Das Wirtschaftswachstum wird durch Normen stärker beeinflusst als durch Patente oder Lizenzen. Normung ist ein strategisches Instrument im Wettbewerb." (http://www.din.de/cmd?level=tpl-bereich&languageid=de&cmsareaid=erfolg_durch_normung).

19 According to Gusy, "Antizipierte Sachverständigengutachten" in Verwaltungs- und Verwaltungsgerichtsverfahren. *Natur* und *Recht* 9 (4) 1987, 164, empirical analysis show the following order: interests of the market leader before others; interests of the industry before others; interests of the providers before interests of the consumers; private interests before public interests; etc.

20 The (criminal) law giver is obviously also influenced by the interest of different lobby groups but still democratically controlled; Burkatzki E (2011) Legalität und Legitimität im Marktkontext. Zeitschrift für Internationales Strafrecht 3, 2011, 162.

needs – specific subsystems such as research, economy, and the health system. It would be inconsistent to rely on these systems on one side and not to accept their specific norms which regulate these subsystems and the interests of its parties on the other[21]. Thus the inclusion of economic interests in standardising procedures does not necessarily lead to their irrelevance for criminal law. Obviously, this acceptance has its limits if the values of the subsystem outweigh society's interests, but the turning point for such specialised norms becoming irrelevant for criminal law is difficult to locate.

Another aspect that could help transferring standards into principles relevant for criminal law is the procedure of developing external standards by non-government institutions. As mentioned, standardising institutions often lack democratic legitimation and transparency.[22]

Why are these considerations important for robotics?

First of all, because there is a very strong activity of standardising institutions in robotics at the moment, thus it seems, from a legal perspective, important to analyse these activities and retie them with legal evaluation. One might even have to consider interaction with the standardising institutions to secure plausible normative premises and processes.

Secondly, the reliance on these standards is also very high: Most researchers and producers are convinced to have acted legally when complying with the existing standards, even if they are somehow vague, not covering all relevant (dangerous) aspects of their activities and normatively questionable. It is necessary to discuss how to connect this strong conviction, supported not just by the official impression of standardising institutions but by the general custom in the actors community, with negligence liability; it might be worth to consider its relevance for the subjective aspects of negligence (guilt). The (potential) "sense of right and wrong" is part of liability for negligence as well.[23] Unavoidable mistake in the lawfulness of the action can therefore lead to negation of negligence. This is the case especially for the parties not directly involved in and profiting

---

21 Steinmann, Unternehmensethik und Recht. Zeitschrift für Internationales Strafrecht (3) 2011, 100-109.

22 For an in depth analysis, see: Gusy, "Antizipierte Sachverständigengutachten" in Verwaltungs- und Verwaltungsgerichtsverfahren. *Natur* und *Recht* 9 (4) 1987, 156–165.

23 OLG Karlsruhe NJW 1967, 2167, 2168; OLG Düsseldorf NJW 1990, 2264 f.; Sternberg-Lieben in Schönke / Schröder (eds.), StGB, § 15 Rn. 193.

from the usage of the robot (researcher, programmer) who are surrounded by a community in which everyone is convinced that fulfilling the requirements of standards is sufficient to act lawfully.

Another condition of criminal negligence is foreseeability of the damage.[24] The more autonomous and potentially dangerous a machine is, the more it can be – generally – foreseen during the research phase that it may, later on, bring harm to humans. The usage of robots for military purposes and the usage of autonomous cars in everyday traffic are plausible examples: It almost seems unavoidable that thereby human beings are (for warfare: unjustifiably) violated. On the other hand: The foreseeability is only connected to the general possibility of harming; the specific conditions and situations become more and more unforeseeable[25]. Robotics is therefore an opportunity to discuss how specific the foreseeability has to be: Does it have to be directed towards specific circumstances, causalities, harms, or is it sufficient to foresee the possibility of violating humans as such?

4. Responsibility – Challenged by Robotics?

The technological development of robotics could even be understood as part of this normative change. Overwhelmed by over complex situations, by everyday life entailing endless risks of damaging third parties, by unforeseeability of already small decisions, we react technologically. In some ways the transfer of responsibility might be the point of these machines: The over-complexity of modern society, in which one has to make numerous decisions every day and knows that many of decisions bear the potential to harm others, leads to building machines not just to decide how to best find our way in traffic or to get our car into a parking spot, not just to remind us about our medicine or buying food – we are building machines to decide about life and death of other human beings. The transfer of the decision only makes sense if the human parties involved are not fully responsible for the decisions. This development has to have consequences for the concept of responsibility as such.

---

24 Lackner /Kühl StGB, § 15 para 46 et seq.
25 Sternberg-Lieben in Schönke / Schröder (eds.), StGB, § 15 Rn. 125.

The adaptive and learning ability[26] of robots necessarily involve a certain degree of unpredictability in their behaviour: Because of the increase of experience made by the robot on its own, the robot's conduct cannot entirely be planned anymore. It also gives more control to the user of the robot than in the case of other products. This leads to the question if every „mistake" by the robot is necessarily caused by a wrongful act of one of the parties in the legal sense[27]. If robots with adaptive and learning capabilities are let free to interact with humans in a non-supervised environment, they could react to new inputs received in an unpredictable way. If a robot then causes damage because of these reactions it is hardly plausible that it was caused by a wrongful act of the programmer, producer or even the user[28].

As mentioned, in cases in which an autonomous robot makes a mistake and thereby damages a third party the traditional negligence regime is – besides missing standards – already confronted with different parties interacting and their interaction probably resulting in future in a machine that acts partly autonomous and can learn from experience; thus the different causes are difficult to impute to one of the parties.

From a general legal point of view, this conflict can, i.a., be solved in the following ways[29]:

- One of the human parties is regarded as generally liable, e.g. the user.[30]
- Only the human party is liable who, provably, made a mistake.

---

26 Günther et al., Issues of Privacy and Electronic Personhood in Robotics, Proceedings of 2012 IEEE International Symposium on Robot and Human Interactive Communication, 2012, pp. 815-820.

27 Boscarato, Who is responsible for a robot's actions? In: B van der Berg, L Klaming (eds) Technologies on the stand: Legal and ethical questions in neuroscience and robotics, 2011, pp. 383–402.

28 Generally about these problems see Leroux et al., Suggestion for a green paper on legal issues in robotics, euRobotics, The European Robotics Coordination Action, 2012.

29 See also Beck, Dealing with the diffusion of legal responsibility: the case of robotics, in: Nida-Rümelin / Bisol (eds.), Technical Options and Ethical-Legal Responsibility, 2014, 167 et seqq.

30 This is how the law handles, at the moment, park distance control systems; Amtsgericht München, Urteil vom 19.7.2007 – Az.: 275 C 15658/07, NJW RR 2008, 40.

- All human parties "behind" the robot can be transformed to a new legal entity.[31]
- One could even, e.g. for social useful robots, transfer the damages onto society itself.

All of these solutions are based on premises about who is profiting from the usage of robots, who should be "punished" financially for its mistake, who is thought to be in control or stay in control even if the machine overtakes some of the originally human decision-making.

But risks in the context of robotics do not only include damages or mistakes: There are also risks of unwanted side effects. Of course, every new technology is accompanied by discussions about slippery slopes. That this is intensively debated in the case of robotics is not surprising: The imagination of robots nursing the elderly or baby-sitting, taking over our everyday communication, giving psychological advice or waging our wars obviously threatens our accustomed perception of the "social"[32]. The probability of change does not necessarily imply that a development has to be restricted or even forbidden. When discussing robotics one has to be aware of the responsibility for these potential side effects, though.[33]

This view onto responsibility problems robotics shall be completed by the already mentioned aspect of the responsibility transfer onto machines[34]. Machines overtaking responsibilities even on the stage of decision making, can, as mentioned, be characterised as technological reaction to the over-complexity of modern society. Behind this development I suspect, besides the hope that machines by having more information and reacting faster than human beings might make less mistakes, the need to hand over these decisions because we feel overwhelmed by the responsibility for them. But this development leads to new questions: Who, then, is the responding entity? Can the machine respond in a way that is neces-

---

31 This obviously does not, by itself, solve all problems and not necessarily exclude the other solutions but gives the third party a kind of adressee, at least for its financial claims. Wettig / Zehendner, The electronic agent: a legal personality under German Law, Workshop on the Law and Electronic Agent 2003, p. 9.

32 Fitzi, Roboter als 'legale Personen' mit begrenzter Haftung. Eine soziologische Sicht, in: Hilgendorf/ Günther (eds.), Robotik und Gesetzgebung, 2013, 377-398.

33 Beck, Dealing with the diffusion of legal responsibility: the case of robotics, in: Nida-Rümelin / Bisol (eds.), Technical Options and Ethical-Legal Responsibility, 2014, 167 et seqq.

34 ibid.

sary for the social and legal construct of responsibility? As we have seen, without such response it will be difficult to establish a new normative structure that will be fully accepted by society.

5. Potential Legal Solutions and Their Consequences for Concepts

General Adaptations in the Risk Society could be to less focus on foreseeability, but more on social adequacy of the action as such, to focus less on external regulations for developing the "standard of care" in a certain area of life but on the legal construction of "admissible risk". This means to negotiate in each area of life if and under which conditions the usage of robots is regarded as such "admissible risk" and if one does act in the adequate framework, one cannot be responsible for the consequences hereof. This also leads to a restriction of the usage of criminal law. In general, it is plausible to not use criminal law too strictly in cases of modern technologies having potential side effects. One also has to be aware that the individual who would be criminally responsible could be heavily overburdened by it. One could pick the driver, the doctor, the user – but he might be the one having to use the autonomous machine (because, for example, his job as taxi driver depending on it), not understanding it sufficiently and being determined in his situative decision, e.g. in traffic, because he could not be as concentrated as if driving himself, and therefore needing more time to react which one does not have in traffic. To be criminally responsible in such situations could be unjust and overburdening.

It also will be necessary to makes some adaptations because of the responsibility transfer onto machines. In general, one increasingly focuses on the „principle of reliance": If different parties cooperate, generally, only the party is criminally liable who provably made a mistake. The other parties can rely on the lawfulness of the other's actions. It is questionable, though, if this principle can be adapted for the responsibility transfer onto machines. These entities are still, in many ways, unknown, unpredictable and uncontrollable. Thus, arguing that one relies on a specific course of action of these machines is hardly plausible. As we have already discussed, it also is not convincing that the user is fully responsible because of his decision to use the machine, because this would render the machines pointless in many ways.

Another solution which is discussed more and more frequently is to transfer the responsibility onto the machine in the legal sense as well, con-

structing a new legal entity, often called the "electronic person". From an inner perspective, it does not pose a big problem for the legal system to reduce individual responsibility in the cases of robots making decisions, to create new legal entities with specific legal responsibilities and to support these changes by strengthening of institutional responsibility in the background, because institutions will decide about the direction of robotics – by financing research, giving out licences, insuring under conditions, etc. But one has to be aware, that by constructing machines who make decisions for us, we give away part of our (social) identity – or maybe better, we reconstruct our identity in a way that it includes machines because we have beforehand decided to use them for a specific part of our autonomy-space.

It has to be discussed further if and how machines or human-machine-hybrids can "respond" for mistakes in a socially acceptable way. It socially is necessary that the entity one makes responsible – morally and legally – has to be able to „respond". This is important not just for the counterpart, the victim, who experiences the human response to its violation and thus might be able to process it in a better way; it also is important for society that there is someone responding to violations normally attributed to humans. This requires, inter alia, some kind of „freedom" – at least from external force, and other normative attributions constructed on the moral and legal premises of each society.

Thus, before adapting the legal system, one has to consider the (potential) changes of fundamental social concepts such as identity, autonomy and personhood. One has to be aware that changing the legal system has as much interdependence with society as social changes do have concerning the regulating laws. Thus, responsibility in the context of robotics includes caution in constructing new entities and changing our normative concepts; this does, of course, not mean that changes are impossible and should be avoided. But they have to be implemented consciously and in awareness of their consequences.

6. Conclusion: What are we discussing?

Discussing responsibility in the context of robotics means more than distributing the financial risks or creating insurances that cover the usage of robots in different contexts. It means to discuss – including society – in which areas of life the advantages of robots outweigh the risks and how

the usage should be created. Thus it is possible to create a so-called "admissible risk", allowing certain actions without being responsible for each unwanted consequence and – most importantly – without overburdening powerless individuals who might have to use the machine without having a choice, who are made the "human in the loop" without being able to make meaningful decisions.

It also means to understand what happens if we intentionally hand over decision making onto machines. It means to legally react on changing fundamental concepts and consciously create the space for these changes. Finally, it means to leave room for decisions against machines taking over responsibility in specific contexts and it means to strengthen the awareness of the relevant institutions who will decide about the development of robotics: They do not only decide about the future of one new technology – in my opinion, they decide about the future of our very basic social concepts, of our understanding of ourselves.

The dilemma of autonomous driving: Reflections on the moral and legal treatment of automatic collision avoidance systems

Eric Hilgendorf[*]

Introduction

The fact that technological progress constantly raises new legal problems is already almost a platitude. Remarkably, however, it seems occasionally to lead to old legal problems reappearing under new guises. A much discussed example currently is the problem of how algorithm-controlled collision avoidance systems, as are used, for example, in modern automobiles, cause their vehicles to react in life-threatening emergency situations. Suppose a vehicle equipped with such a system approaches an accident scene. Three severely injured accident victims, A, B and C lay unconscious on the road, but victim D was able to drag himself to the side of the road and is grasping a sign post to stay on his feet. A second vehicle is approaching the scene. It is moving too fast to stop. It is also not possible for it to swerve in such a way as to avoid striking A, B, C and D. How should the onboard computer steer the car? The attractiveness of such hypothetical cases is due not least to the fact that they help to illustrate the basic values of a legal culture, in a manner which is also accessible to a broader public. Proposed solutions sometimes take on the character of legal and social policy decisions[1].

In this contribution, a proposal to deal with the above mentioned problem will be developed that meets practical requirements, but at the same time is consistent with German legal doctrine. Towards this end, the no-

---

* Prof. Dr. Dr. Eric Hilgendorf, Julius-Maximilians-Universität Würzburg.

1 In the current debate, the decision-making problem sketched out above is often reduced to the opposition "Kant vs. Bentham", especially in more popular representations, which, however, certainly remains inadequate because of the chauvinistic Germanic undertones of many such comparisons. For the political-historical dimension of the distinction between "German culture" (Kant), "shallow" French "civilization" (Voltaire) and the "utilitarian merchant spirit" of the British (Bentham), see Hilgendorf, "Rechtsphilosophie der Aufklärung" in Hilgendorf & Joerden (eds.), *Handbuch der Rechtsphilosophie*, 2017, p. 137 *et seq*.

tion of *degrees of wrong* will be introduced and the already established legal concept of *accepted risk* will be extended to automatic technological systems.

I. Automated driving and the law

The ethical and legal issues that have arisen in the context of automatic collision avoidance systems in motor vehicles have become an important issue in the debate on the future of road transport in Germany[2]. The new possibilities provided by automated driving are should definitely be rated positively overall – one need only consider benefits such as mobility gains for the elderly and the disabled, improvements in road safety, environmental protection, energy efficiency and an increase in the ease of transport[3]. It would therefore be wrong to view automated driving from the outset with skepticism or to reject it. The law should not block, but rather should steer and promote the development of important new technologies; According to the view represented here, technology law should therefore not be an instrument for preventing innovation, but rather for supporting (and promoting) innovation.

It is obvious, however, that automated driving poses a multitude of difficult and unresolved legal problems. This applies to international law (in particular the Vienna Convention on Road Transport, 1968), as well as national constitutional law, civil liability law, criminal law, data protection law, technical approval law, and insurance law[4]. In this article I will try to analyze a particularly controversial problem at the interface between

---

2 The starting point of the current debate were articles by the American philosopher of technology Patrick Lin, cf. for example Lin, *The Ethics of Saving Lives with Autonomous Cars is Far Murkier than you Think* (https://www.wired.com/2013/07/the-surprising-ethics-of-robot-cars); Lin, "Why Ethics Matters for Autonomous Cars" in Maurer *et al*. (eds.), *Autonomes Fahren*, 2015, pp. 69 – 85. Cf. also Bonnefon, Shariff & Rahwan, *Autonomous Vehicles Need Experimental Ethics: Are We Ready For Utilitarian Cars?* (https://www.researchgate.net/publication/282843902_Autonomous_Vehicles_Need_Experimental_Ethics_Are_We_Ready_for_Utilitarian_Cars); dies., The Social Dilemma of Autonomous Vehicles (Science on 24 Jun 2016: Vol. 35, DOI: 10.1126/science.aaf2654).

3 Hilgendorf, "Gutachten zum Thema 'Automatisiertes Fahren und Recht'" in *53. Deutscher Verkehrsgerichtstag 2015*, 2015, pp. 55 – 72 (57 *et seq*.).

4 Cf. also the overview in Hilgendorf, *op.cit.* 2015 (Fn. 3). p. 59 *et seq*.

ethics, constitutional law, criminal law and civil law, namely the question of which rules may or should be incorporated into automatic collision avoidance systems[5]. What we are dealing with here are systems of rules that enable the on-board computer of a vehicle to avoid an obstacle in the direction of travel, and this is done by the vehicle much faster than would be possible for a human being, who, in such a situation, can neither assimilate the necessary information quickly enough nor turn in time to change the trajectory of the vehicle to avoid a collision.

The new collision avoidance systems are likely to contribute to a reduction in the number of road traffic accidents. They will, however, also cause accidents if swerving vehicles are steered towards targets that would not have been hit in the absence of the computer directed evasive maneuvers. In this respect, the situation is similar to what happened when airbags or seatbelts were first introduced. That was also highly controversial at the time, since the devices do not merely save lives and prevent injuries, but in a small number of individual cases can cause injuries or deaths[6].

Of course, collisions occur in road traffic today, including those involving injuries or even deaths. Human car drivers are frequently overwhelmed in collision situations and can then no longer make well thought out decisions. This is also one reason why collision scenarios in road traffic have so far hardly been analyzed either from ethical or legal perspectives. The new possibilities offered by technology compel us to consider and analyze the relevant processes and sequences of events. One could even say that a *compulsion to analyze and to explicate* exists in association with the development of algorithms, which, in parallel with the introduction of new autonomous systems, is impacting the way we live and work. Sequences of events that previously were more or less uncontrolled, and indeed unfolded in an uncontrolled manner, can now be decompiled into individual elements and processed in a structured way using algorithms. They can then be steered and controlled.

As (causative) factors relevant to collisions become more transparent and more controllable, responsibility arises, namely both in moral and le-

---

5 The entirety of implemented rules constitutes a system of norms which for human beings could be characterized as a “fundamental moral orientation”.

6 Bergmann, “Die Gurtdebatte der 1970er und 1980er Jahre in der BRD” in *Technikgeschichte* vol. 76 (2009), pp. 105 – 130; cf. also Forschungsgemeinschaft Der Mensch im Verkehr (ed.), *Für und Wider Sicherheitsgurte*, 1973. See also http://www.spiegel.de/einestages/einfuehrung-der-gurtpflicht-a-946925.html.

gal terms. It cannot be avoided by refusing to use automatic collision avoidance systems entirely or in certain accident situations, programming the computer to make random decisions – the decision not to make a decision is also a decision which creates responsibility[7].

In emergency situations in which an actor cannot avoid violating one (of at least two) legal interests, the *principle of the lesser evil* applies fundamentally in our legal system[8]: damage caused must be kept as low as possible. If the killing of one or more human beings can only be avoided by damaging someone's property, the property damage is justified. The same rule applies in the hypothetical road traffic dilemma discussed above: if a car is involved in a potential accident situation in which it is about to run over several seriously injured people lying on the road, it is imperative that the car swerve to avoid hitting those people even if it then, for example, causes property damage to a sign post, or to a parked car, or to objects standing at the side of the road. The value of the damaged chattels pales in significance – human lives are always more important than things according to hierarchy of values of our legal system[9].

The principle of the lesser evil becomes problematic, however, when the life of one human being is pitted against the physical integrity or even the life of another human being. What we are confronting here is a fundamental legal and ethical problem involving collision avoidance systems. How should the system decide when one life is pitted against another? Who should live and who should die? There are a range of similar hypo-

---

7 The concept of responsibility used here can be visualized in the following way: Person X is responsible for an event Z under rule Y. If one accepts this, then among other things it becomes clear that only persons can be responsible for violating a rule. The (socially determined) consequences of an attribution of responsibility can be manifold; their most important manifestations in the law are civil liability (a duty to pay compensation for damage incurred) and criminal liability, that is, the commission of all the elements of a criminal offence, so that conviction and punishment may follow.

8 The most important expression of this principle in German law are the rules governing necessity in the criminal law (§ 34 StGB), under which the protected interest must "significantly outweigh" the interest interfered with.

9 Moreover, there is much to be said for not merely classifying chattels according to their monetary value, but rather also taking into account other considerations, for example with respect of works of art (Michelangelo's Pietà) or animals (we have all heard that some people love their pet more than any human being). In both cases, there are already laws (for example, the Copyright Act for Art and Photography, the Animal Protection Act) which distinguish these chattels from other chattels.

thetical situations discussed in the ethics literature, each with its own name, such as "the plank of Carneades[10]", "castaways on the high seas"[11], "euthanasia of the mentally ill during the Third Reich"[12], "the switchman's case"[13] and "the trolley problem"[14]. Of particular practical relevance in this context is the decision of the German Federal Constitutional Court (2006) on the Aviation Security Act (*Luftsicherheitsgesetz*) [15]. At issue was the question of whether a commercial airliner filled with innocent passengers[16], which had been hijacked by terrorists with the intent of using it as a weapon of mass destruction, for example, by crashing it into a

---

10 On this subject cf. Hilgendorf, "Tragische Fälle. Extremsituationen und strafrechtlicher Notstand" in Blaschke *et al.* (eds.), *Sicherheit statt Freiheit? Staatliche Handlungsspielräume in extremen Gefährdungslagen*, 2005, S. 107 *et seq*.

11 Mitsch, "'Nantucket Sleighride' – Der Tod des Matrosen Owen Coffin" in Heinrich *et al.* (eds.), *Festschrift für Ulrich Weber*, 2004, p. 49 *et seq*.; Simpson, *Cannibalism and the Common Law*, 1984; Ziemann, *Zeitschrift für international Strafrechtsdogmatik* 2014, p. 479 *et seq*.

12 OGHSt 1, 321; BGH, *Neue Juristische Wochenzeitschrift* 1953, p. 513.

13 A railway car rolls down a sloping section of track toward a group of five railroad workers. A switchman can save the lives of the five railroad workers only by redirecting the car onto a side rail where there is a person standing, who will be struck and killed by the car. Can the switchman lawfully redirect the train? This problem, which has been discussed in many different variations, can be traced back to Welzel, *Zeitschrift fur das Strafrechtswissenschaft* 63 (1951), p. 47 (51). But switchman cases may also be found in older criminal law writings, e.g. by Köhler, *Der Notstand im künftigen Strafrecht*, 1926, p. 45 comment 1.

14 In 1967 the British moral philosopher, Philippa Foot, discussed the switchman problem in her article "The Problem of Abortion and the Doctrine of the Double Effect", *Oxford Review* 5 (1967) pp. 5 – 15. Since then, what is known by the name "trolley problem", has been a core element of Anglo-American moral philosophy, most recently, for example, in Edmonds, *Would You Kill the Fat Man? The Trolley Problem and What Your Answer Tells Us About Right and Wrong*, 2014; Kamm, *The Trolley Problem Mysteries*, edited and introduced by Eric Rakowski, 2016; Cathcart, *The Trolley Problem or Would You Throw the Fat Guy Off the Bridge? A Philosophical Conundrum*, 2013.

15 BVerfGE 115, 118 *et seq*.

16 Below, the terms "innocent" or "innocent person" are used as non-technical descriptions for the designation of two classes of persons. Firstly those who are free of moral wrong or are not culpable so that there is no reason why they should be subjected to or bear special risks, for example of being injured or killed, as would be the case in the course of being judicially sanctioned or punished. Secondly, a class of persons who have not assumed special risk of injury in the performance of their professional duties, for example soldiers, police, fireman, etc.

city centre, could be shot down. In its decision, the court rejected the idea that the airliner could be shot down. The court primarily reasoned that such a course of action would violate the human dignity of the aircraft's passengers. It held that it was unconstitutional for human lives to simply be "weighed against one another"[17].

The dilemma of sacrificing lives in order to save other lives has been discussed in philosophy and jurisprudence since antiquity, without a definitive answer being found. There exists today a vast range of literature[18], nearly overwhelming in its sheer volume, even for experts, which could be a fruitful resource for developing solutions to present problems. It is certainly not the case that the problem should be seen as resolved. In particular, the decision of the Federal Constitutional Court cannot be viewed as the final answer in the debate on conflicts of the type "balancing lives against lives" in emergency situations. Particularly in the criminal law, many questions are still unresolved[19]. It would be equally incor-

17 The shooting down of a passenger plane would be a violation of Article 1 (1) GG as well as the prohibition of killing which derives from it. "This does not change the fact that this approach is intended to protect and preserve the lives of other people." On this subject (written before the BVerfG decision), see Lindner, *Die Öffentliche Verwaltung* 2006, p. 577 *et seq*.

18 In addition to the texts cited in footnotes 10 – 17, cf. Archangelskij, *Das Problem des Lebensnotstandes am Beispiel des Abschusses eines von Terroristen entführten Flugzeuges*, 2005; Bott, *In dubio pro Straffreiheit?,* 2011; Coninx, *Das Solidaritätsprinzip im Lebensnotstand*, 2012; Fritze, *Die Tötung Unschuldiger*, 2004; Ladiges, *Die Bekämpfung nicht-staatlicher Angreifer im Luftraum*, 2008; Merkel, *Juristenzeitung* 2007, 373 *et seq*.; Mitsch, *Goltdammers Archiv für Strafrecht* 2006, 11 *et seq*.; Pawlik, *Juristenzeitung* 2004, 1045 *et seq*.; Roxin, *Zeitschrift für internationale Strafrechtsdogmatik*, 552 *et seq.*; Sinn, *Neue Zeitschrift für Strafrecht* 2004, 585 *et seq.*; Stübinger, *Notwehr-Folter und Notstands-Tötung*, 2015; Wilenmann, *Zeitschrift für die gesamte Strafrechtswissenschaft* 127 (2015), p. 888 *et seq*.; Zimmermann, *Rettungstötungen*, 2008; Zoglauer, *Tödliche Konflikte. Moralisches Handeln zwischen Leben und Tod*, 2007. Even in older writings, cases of "life-balanced against-life" decisions, in the context of emergencies, were only rarely regarded as justified, cf. Klefisch, *Monatsschrift für Deutsches Recht* 1950, 258. For more on the legal history of how this problem has been dealt with in German legal doctrine, cf. Wilenmann, *Zeitschrift für die gesamte Strafrechtswissenschaft* 127 (2015), p. 888 (893 *et seq*.). For Anglo-American writings on the "trolley problem" compare the citations above in Fn. 14.

19 Quite rightly Schneider wrote in *Münchener Kommentar zum StGB*, 2017, preliminary remarks on § 211 *et seq*., paragraph 29: "The criminal law principles of the prohibition on the quantification and qualification of human life, as well as the in-

rect to give up on the problem as practically irrelevant or unsolvable, and to push it to the side with a shrug of the shoulders.

II. Ethical and legal guidelines as well as a proposed solution

1. "Setting off" human lives vs. a humane orientation in the law

If it was allowed to "set off" human lives against one another, one could argue that it would be permissible to kill an innocent person, if only in that way could the lives of several other (i.e. more) people be saved[20]. This would mean, for example, that a vehicle approaching an accident situation at high speed and threatening to kill two severely injured people lying on the road, could or even should swerve to avoid running over those injured persons, even if another person was killed by the evasive maneuver (e.g. someone walking along the side of the road). The justification for programming a system to do that, would, however, contradict a principle inherent in humanely oriented legal systems, namely that human beings and their dignity constitute the "highest value"[21]. This excludes the possibility of "setting off" human lives against other human lives, according to the overwhelming view in German legal science and court jurisprudence[22].

---

commensurability of the value of life, are among the frequently highlighted but rarely verified basic convictions of criminal law practice and criminal legal science."

20 This position is often attributed to utilitarianism, but as a rule no particular representative of this school of thought is named. A strict "set-off solution" would probably be justified from the viewpoint of a less reflected act utilitarianism, but in contrast would not be justified from the perspective of rule utilitarianism. Utilitarian arguments are usually much more sophisticated than is characterized in discussions by German speakers. For a provocative treatment, cf. Peter Singer, *Neue Zürcher Zeitung* 24.5.2015, who even wants to "set off" the lives of pigs against the lives of human beings (http://www.nzz.ch/nzzas/nzz-am-sonntag/philosoph-peter-singer-ein-embryo-hat-kein-recht-auf-leben-1.18547574). This suggestion violates two taboos: setting off lives against each other and weighing human lives against animal lives.

21 The concept of "highest value", like the word "innocent" (footnote 16), needs clarification. It is used here to describe the notion that the legal order is intended to serve the individual whose dignity cannot yield to any other exigency such as "people", "class" or "will of the God".

22 OGHSt 1, 321 (334); BGH, *Neue Juristische Wochenzeitschrift* 1953, 513 (514); BGHSt 35, 347 (350); Kühl in Lackner & Kühl, *Strafgesetzbuch*, 2014, § 34 StGB,

On the other hand, it would be very difficult, both morally and legally, in emergency situations, in which the killing of innocent people cannot be avoided, not to try to injure as few innocent people as possible. Therefore, a quantification of victims hardly seems avoidable. In any case, it would not be morally convincing to assert that morally there is no difference between the killing of one innocent person, or respectively, the killing of several or even many innocent people. Suppose a misanthropic programmer wrote a collision algorithm so that his vehicles always killed the largest possible number of people in "set off" situations. Such an algorithm would hardly be regarded as morally acceptable, because we intuitively demand that the number of innocent people killed be kept as low as possible. Perhaps even more counterintuitive would be a system which, appearing to follow the principles that lives cannot be set off against each other and that the destruction of one innocent life is just as "bad" as the destruction of very many innocent lives, was programmed with an algorithm so that in potential accident situations the vehicle killed the lowest possible number of people when it was south of the Main River (i.e. within Bavaria), but in contrast killed the largest possible number of people when it was north of the Main River (outside Bavaria). Such a "Bavaria friendly" collision algorithm should get even the most stubborn set off skeptics to start ruminating[23].

On the basis of legal humanism[24], it appears necessary to keep the number of victims as low as possible in cases of the unavoidable killing of innocent people. Therefore if an automatic collision system is faced with the choice between killing one or several innocent people, in a situation where an accident is unavoidable, the avoidance system should choose the solution in which only one, and not several, persons are hit by the car. It is likely that this result will correspond to the moral intuition of most people,

---

paragraph 7; Perron in Schönke & Schröder, *Strafgesetzbuch*, 2014, § 34 StGB, paragraph 23; Roxin, *Strafrecht AT I*, § 16 paragraph 29; Welzel, *Zeitschrift für die gesamte Strafrechtswissenschaft* 63 (1951), 47 (52); cf. also Ladiges, *Juristische Schulung* 2011, p. 879 (882 *et seq*.), who discusses the problem in the context of "legal justifications" for killing a human being.

23 If one analyzes the reasons for our intuitive rejection of such an algorithm, one major factor seems to be the fact that using geographic location as the distinguishing criterion violates our notions of human equality, that is, it is an unacceptable or invalid criterion.

24 Hilgendorf, "Humanismus und Recht – Humanistisches Recht? Eine erste Orientierung" in Groschopp (ed.), *Humanismus und Humanisierung*, 2014, pp. 36 – 56.

that is, prevailing social ethics. It still needs to be investigated whether this principle can stand as it is, or whether it needs further refinement.

2. A proposed solution: Degrees of wrong

According to the view developed here, the killing of innocent people should always be unlawful, even in emergency situations. Let's go back to the hypothetical situation we discussed earlier. Please recall that a car with an automatic collision avoidance assistant was rapidly approaching an accident site, in which three persons had been thrown out of a car and lay seriously injured on the ground. One person was able to drag himself to the side of the road and was leaning on a sign post. The approaching vehicle faced the "decision"[25] either to stay in its lane and run over the three injured people, whereby it would have been very likely that all three of them would be killed, or to swerve to the right and kill the fourth person standing at the roadside. If that happened, a human driver would not be able to rely on the justification defence contained in § 34 German Criminal Code (*Strafgesetzbuch* – StGB): the emergency situation – the expected outcome of killing the three injured people on the ground – cannot be legally avoided by changing the trajectory of the car so that it then causes the death of the individual standing at the roadside. An assessment of the legal interests of the parties, based on what has up to now been prevailing legal opinion, would determine that the one protected legal interest, i.e. the lives of the three injured persons, did not significantly outweigh the other legal interest, which would be prejudiced by the maneuver, i.e. the right to life of the individual who would be killed[26]: Even three lives do not "count" for more than one life when legal interests are balanced, since each individual life in and of itself represents the highest possible maximum value. It should be noted that, strictly speaking, this result was not achieved by prohibiting the balancing of "lives against lives", but rather

---

25 Once again, the question has arisen whether a hitherto anthropocentric vocabulary can easily be applied to machines ("autonomous actors"). On this subject, cf. Hilgendorf, "Können Roboter schuldhaft handeln? Zur Übertragbarkeit unseres normativen Grundvokabulars auf Maschinen" in Beck (ed.), *Jenseits von Mensch und Maschine*, 2012, pp. 119 – 132.

26 This is the almost unanimous view, cf. Kühl in Lackner & Kühl, *op.cit*., 2014, § 34 StGB, paragraph 7.

by stressing one very specific consideration: No life counts more than any other life, and even the lives of many persons cannot be classed as more valuable than the life of a single individual. From a humanist perspective, the individual and his rights are the guiding values in our legal order, so that as a matter of principle it is not permissible to oblige the individual to sacrifice his life or other basic rights for the benefit of others[27], that is to say, to tolerate being killed or being the victim of serious bodily harm in the furtherance of the interests of others.

The orientation towards the life of the individual as a "non-balanceable highest value" can be explained by the fact that after 1945, the drafters of the German Constitution consciously chose man and his individual dignity as the point of reference and goal of the entire legal system[28]. This is especially clear from the sentence which was proposed as the first sentence of the Article 1(1) of the draft constitution at the Herrenchiemsee Constitutional Convention (10-23 August, 1948): "The state exists for the people, not the people for the state."[29] The human orientation of law, expressed in this way, is an essential element of the approach to the rule of law established in the German Federal Constitution. The principle of human orientation has been developed into a "humanist imperative" in our law: Na-

---

27 For an apt treatment, cf. Erb, *Münchner Kommentar zum StGB*, § 34 paragraph 116, 2017, with additional citations, who discusses the "absolute limits of a duty" to sacrifice one's own life for the benefit of others and rightly wants to apply this principle to "serious health problems". For arguments in the same direction, cf. Frister, *Strafrecht Allgemeiner Teil*, 2015, chapter 17 paragraph 15; Wilenmann, *Zeitschrift für die gesamte Strafrechtswissenschaft* 217 (2015), p. 888 (909).

28 Life is for this reason unpredictable, because the acceptance of substantial losses of rights in respect of formally protected legal interests cannot be demanded of citizens, except where they are responsible for those losses. For the rules which permit invasions (exceptions) to protected legal interests must be justifiable from the perspective of the individual "(written so concisely by Wilenmann, *Zeitschrift für die gesamte Strafrechtswissenschaft* 127 (2015), p. 888 (909)).

29 Quoted after Dreier, *Grundgesetz Kommentar*, 2013, Art. 1 (1), paragraph 23. Translation by W. Schäubele, "The Herrenchiemsee Constitutional Convention 60 Years On", a speech held by the Interior Minister on 7.20.2008. It must be pointed out, however, that the GG and its interpretation by the Federal Constitutional Court also includes approaches, which relativize the orientation of the legal order towards the individual, by means of the concept of "community-relatedness" (i.e. public welfare), cf. BVerfGE 4, 7 (15). For more detail on the unpredictability of reference to the "image of mankind" in the GG, see Hilgendorf, "Konzeptionen des 'Menschenbilds' und das Recht" in Joerden *et al.* (ed.), *Menschenwürde und Medizin. Ein interdisziplinäres Handbuch*, 2013, p. 195 – 216 (203 *et seq*.).

tional law has to ensure that despite all societal, economic, scientific and technological developments, the individual human being remains the centre and starting point of the entire legal system.

The significance of this humanistic postulate becomes clearer if one compares it with conceptions of the state present in other forms of government: In a *theocracy*, man, with his needs and wants, is not at the centre of the law, but rather it is the will of the deity, which lays claim to obedience to its precepts even when they are associated with the greatest possible human suffering. Man is no more than a "slave of God"[30]. Another decidedly non-humanistic form of government is the totalitarian dictatorship, following the Stalinist or National Socialist model, in which the rights of the individual are completely suppressed. As a rule, totalitarian governments try to legitimize themselves by citing overarching and pressing national needs (reasons of state) or the needs of the collective ("It is good to die for the Fatherland", "You are nothing, your people are everything")[31].

In contrast, according to our current humanistic legal understanding, which from the rise of Humanism in the 16th century up to the Enlightenment of the eighteenth century largely gained acceptance in Europe, the individual, with his dignity and his "innate" human rights, is at the centre of the legal order. In modern times, this position was formulated for the first time in the early 16th century by authors such as Pico della Mirandola[32]. Of course in intellectual history terms, it can be traced all the way back to the Greeks and Romans of antiquity[33]. This central position of the individual would be jeopardized if the life of one person could easily be set off against the lives of others in emergency situations. The prohibition on setting off lives against each other is based on considerations of principle, which do not change, even where large numbers of lives are at stake. Thus an individual human life cannot be balanced against the lives of 100, 1,000 or 100,000 other people; killing one to save the many is still unlaw-

---

30 On this theme, which is found both in Christianity and in Islam, cf. Hattenhauer, "Die Sklaven Gottes" in Finkenauer (ed.), *Sklaverei und Freilassung im römischen Recht, Symposium für Hans Josef Wieling zum 70. Geburtstag*, 2006, p. 59 – 82.

31 Regarding the latter, cf. Stolleis, *Gemeinwohlformeln im nationalsozialistischen Recht*, 1974.

32 Pico della Mirandola, *De hominis dignitate, Über die Würde des Menschen* (1496), 1990 (Philosophische Bibliothek vol. 427).

33 Cancik, "Freiheit und Menschenwürde im ethischen und politischen Diskurs der Antike" in Cancik (ed. Cancik-Lindemaier), *Europa – Antike – Humanismus. Humanistische Versuche und Vorarbeiten*., 2011, p. 175 – 189.

ful. However, in the case of people who are confronted with such horrible decisions, their unease will grow as the number of innocent victims rises, and ultimately, they will indeed decide to kill the lesser number of victims. This psychological reaction can be taken into account in the criminal law by a legal exculpation: the action is illegal, but where the danger cannot be avoided in any other way, the actor incurs no criminal liability under the defences of exculpatory emergency (§ 35 StGB) or extra-statutory exculpatory emergency[34].

An argument against the basic position represented here could be seen in the fact that it is based both on a particular conception of human nature which was developed in Europe, as well as on specific understanding of human dignity; it is not intuitively obvious and may require more detailed and compelling reasons. This objection, which is often found in the philosophical debate on human dignity[35], strikes the issue at its core. The idea of man as a unique creature endowed with dignity, is a product of the European intellectual history which began in ancient Greece: the pointed emphasis on human dignity after World War II, which among other things was expressed in the prohibition against setting off human lives against each other, was a reaction to the unprecedented crimes against humanity committed under National Socialism in Germany (and Stalinism in the Soviet Union). It does not follow from the historically very specific way in which this particular conception of human dignity emerged, that it is necessarily correct or valid. Of course the values expressing themselves in the

34 Necessity not envisaged by the law, for example, was pleaded as a defence in criminal proceedings to charges of murdering mentally ill patients during the 3rd Reich; the heads of asylums claimed that they had let a certain number of innocent patients be killed in order to save a considerably larger number of patients (see the references in Fn. 12). In its decision on the Air Safety Act, the Federal Constitutional Court alluded to a similar solution in the case of a passenger aircraft hijacked by terrorists, which would be shot down by the German military before reaching the intended location at which it would be used as a weapon of mass destruction. This result was dealt with in a literary context in Ferdinand von Schirach's play *Terror* (2015), whose treatment of the legal issues, however, was not entirely convincing. After the broadcast of the filming of the play on 17.10.2016, according to press reports, about 86% of the viewers voted for "acquittal" of the soldier performing the execution. For criticism of Schirach's play from a legal perspective, cf. Schild, *Verwirrende Rechtsbelehrung, Zu F. von Schirachs 'Terror'*, 2016.

35 Hilgendorf, "Menschenrechte/Menschenwürde" in Cancik *et al.* (ed.), *Humanismus: Grundbegriffe*, 2016, p. 275 – 288 (285 *et seq*.).

"prohibition on setting off lives" are an essential aspect of a humanistic understanding of the law, which has been put forward since the Enlightenment with the claim of having universal validity. This conception was taken up in the German Federal Constitution (1949), and, as enshrined in Art. 1 GG, it is a mandatory rule of our constitutional order.

If the killing of innocent people is always unlawful on the basis of a humanist understanding of the law, the question arises as to how the idea of minimizing the number of lives lost, as above, can be justified in cases where life inevitably is at stake. According to our view, in cases where the dilemma of "weighing life against life" arises, when a decision has to be made between the destruction of one life and the destruction of another life, the principle of the lesser evil must always be followed: if innocent people must die, then it should be as few as possible. If nothing else, this follows from the superior position of the individual developed above. Otherwise, we would consider the two surplus lives, so to speak, as a *quantité negligeable*. The killing of every innocent person remains wrong and cannot be justified. One ought, however, apply the notion of *degrees of wrong*[36], which dictates that one should put as few lives as possible at risk, or indeed cause as few deaths as could be possible.

This position can be illustrated by the following hypothetical example: During an airplane crash, the pilot can either steer the plane so that it crashes over a nearly uninhabited area (so that only he himself and all his passengers plus a few people on the ground are killed) or steer it so that the machine crashes over a densely populated area so that not only everyone on board the plane is killed, but also a few hundred or a thousand people on the ground will almost certainly be killed. According to the approach outlined above, the pilot not only has a moral duty but also a legal duty to steer the plane so that the crash takes place over the sparsely populated area. The argument that when human beings are killed every quantification or balancing of lives is impermissible, because there is no normatively relevant difference between the killing of a few persons or many persons, is not convincing because it reduces human life to a *quantité negligeable*. Every human life counts! It remains the case that the killing of innocent human beings is not condoned by the legal system, but rather is classified as a wrong. It follows that the potential victims on the ground

36 Hilgendorf, "Recht und autonome Maschinen – ein Problemaufriß" in Hilgendorf & Hötitzsch (eds.), *Beiträge der 1. Würzburger Tagung zum Technikrecht*, 2015, pp. 11 – 40 (26).

would retain a right of self defence in the moments prior to the crash. On their part, it would be lawful, therefore, if they tried to shoot down the approaching aircraft.

3. *Use of deadly force in especially grave emergency situations involving or not involving risk communities*

Looking at the issue of "risk community", it is necessary to discuss what role it can or should play that the persons who are at risk, or are threatened, all equally face the same risk. *Gefahrengemeinschaft*, which translates as "risk community", is a term in use in German law. It is defined as a group of persons facing a certain risk, which may be aware that it is facing that risk. Such a situation would occur, for example, when in heavy rush hour city traffic three children A, B and C suddenly jumped in front of a vehicle in such a way that, without the car being able to swerve, two of the children (A and B) would be hit by the car's right fender, but the other child (C) would be hit by the left fender. Had the driver had been able swerve the car, he could have steered it to hit either A and B, or C (it was not possible to completely avoid the accident by braking or swerving).

In situations where a risk community exists, as described in the previous paragraph, it must first of all be stressed again[37] that neither the killing of A and B nor the killing of C can be justified. Nevertheless, the question still arises as to whether the car should simply drive straight forward, without swerving – then hitting all three children – or swerve to the right, resulting in a collision with A and B, or swerve to the left with the consequence of a collision (only) with C. It seems to me that this hypothetical problem certainly provides support for making decisions based on degrees of wrong[38]: it is ethically and legally necessary in order to minimize the injuries caused to swerve the car hit C rather than A and B, if the same probabilities of injury and severity of expected injury are present (death, severe bodily harm). Simply invoking "destiny" or the "will of God" as a justification for driving straight ahead and killing all three children seems just as unconvincing as making a decision based on spurious criteria such

37 See above, p. 65 et seq.
38 See above, Fn. 36.

as age, gender or skin color. It would be equally absurd to swerve so that A and B would be struck and killed, for example using the argument that human lives cannot be quantified or balanced against each other, and therefore it does not (from a normative perspective) make any difference whether one, two or three children are killed.

Not convincing (but possibly sustainable) would be calls that a random number generator be used to make the decision on behalf of the programmer. But suppose the random decision was that all three children be killed, although two of them could have been saved – would such a decision be compatible with the fundamental values of our legal system? And who could convincingly make the case to the parents that it was the right decision? Moreover, failure to devise an algorithm based on a hierarchy of outcomes, contains the implicit decision, for which we are responsible, that the result should be left to chance. Finally, it would also be conceivable to open up the possibility for each respective driver to determine in advance how his vehicle will behave in collision scenarios, such as those discussed here, within a range of predetermined possible outcomes. It is obvious, however, that the ethical and legal problems discussed here have not been resolved, but only put off for later.

It should be borne in mind that according to the linguistic usage proposed here, a risk community not only exists when the legal interests concerned have already been massively and specifically put at risk. It is sufficient if the affected legal interests were in principle put at the same risk. One might therefore call it a "symmetrical risk community".

It still needs to be settled how cases will be dealt with where the potential victims of the collision, at the point in time when the computer system makes its decision, do not face the same risks (i.e. there is no risk community). This would be the case, for example, where the car is approaching a group of three seriously injured people (lying on the street) while a single individual is standing at the side of the road, who would certainly be struck and killed if the vehicle swerved to avoid the persons lying on the road[39].

According to the approach presented here, there is no justification for the killing of innocent persons, no matter what decision the system makes. Whatever transpires will be wrong. If one assumes that the risk of being killed is the same both for the three persons lying on the road and for the

39 See above, p. 57.

single individual standing at the side of the road, then one could once again argue that the principle, by which the greatest possible number of innocent persons should be saved, ought to be adhered to so that the vehicle should swerve to avoid the three severely injured people in the road, thereby killing the individual at the side of the road. But that would ignore the fact that before the computer made its decision, the chances of survival were not equally distributed. The vehicle was driving towards the three severely injured people on the road. It only threatened to kill them. If the vehicle is caused to swerve, then the chances of survival are being changed (redistributed). In accordance with social morality (which is not quite clear in this case[40]), there is much evidence here that such a redistribution of the chances of survival should be regarded as incompatible with the humanistic principle of an orientation to the human being as a maximum value of our legal order. The final result of this case is significantly different from that of the risk community, in which all legal interests concerned faced the same risk before the decision was made by the computer[41]. In the instant scenario the algorithm should therefore be designed so that the vehicle does not swerve[42].

III. The quantification of human life in current applicable law

The position developed here contradicts the often somewhat thoughtlessly made assertion in Germany that human life cannot be quantified or at least

---

40 In the context of the trolley problem, the variant discussed here would probably correspond to the "fat man problem", cf. Edmonds, *Would You Kill the Fat Man? The Trolley Problem and What Your Answer Tells Us About Right and Wrong*, 2014, p. 35 *et seq*.

41 In the airplane scenario as well, one could well assume "normatively equal" risks, if the aircraft was still far away from possible crash targets.

42 The present paper does not deal with problems of evidence and computer errors. In order to avoid evidential difficulties, black boxes should be installed in all vehicles with high degrees of automation. Computer errors also present an interesting problem: What are the legal consequences, when a computer incorrectly records or misinterprets data? Instead of a disparity between "imagination and reality", the discrepancy here is between "internal representation and reality". In the present state of AI research, however, there seems to be good reason to ignore factual errors and mistakes of law by machines, since categories such as "wrong" and "guilt" can hardly be applied sensibly to machines. Cf. sources referred to in Fn. 25.

must not be quantified. In the former assertion, the proposition is obviously wrong: the fact is that human life can be quantified. Anyone can see that this is so by counting the number of living people in a group of human beings, that is, determining their quantity. What is meant by the proposition is not that it is factually impossible to quantify human beings, but rather that it should be forbidden without exception: human lives *should* not, and *must* not be quantified in contexts in which the killing of human beings is an issue under discussion.

There also exist *de lege lata* areas, in which a quantification of human life is permitted, or indeed even required. One example would be sentencing (§ 46 StGB) or aggravating factors at sentencing as under § 306 b (1) StGB. It should be obvious that the sentence imposed by the court will be different where the offender has killed one or many people. This is an issue which must be addressed during the sentencing procedure. We may even go one step further and say that the more people who have been killed, the longer will be the sentence imposed on the offender by the court. A second, and less clear area in which quantifying considerations may play a role is conflicting duties, for example in cases where only one or more persons can be rescued at the cost of others being sacrificed. Let's look at a hypothetical case: a lifeguard has to choose between rescuing child A or rescuing the group of children B, C, and D. Should he not be required to save the group of children rather than the individual child? This question has not yet been conclusively resolved in German legal doctrine.[43]

A further area in which the quantification of human life is permissible is within the context of the application of the principle of proportionality. Let's look at a hypothetical example: a necessary police operation can be carried out in two equally effective ways, a and b. In operation a, the life of only one person who is not involved would be endangered, but in operation b the number of innocent people put at risk is five. It seems obvious that a quantification of the human lives put at risk by the respective operations, is not only permissible but must be conducted. Should not the same also be true when the innocent people are not only put at risk, but where it is certain or nearly certain that some of them will be killed? A quantification of human life also appears to be necessary, not where innocent people are involved, but where perpetrators will be affected or killed. If the police

43 Cf. Merkel, *Juristenzeitung* 2007, 373 (380).

have various different ways of preventing a terrorist attack (in which innocent people would be killed), they cannot simply kill all the terrorists (by dropping a bomb on them), but must choose the safest measure, i.e. the one which harms or kills the lowest number of victims possible, even if the victims are terrorist attackers. Such an operation would therefore only be legal if conducted in the way least likely to cause lives to be lost (possibly having quantified and compared the possible numbers of victims likely to be caused in the various scenarios under consideration).

Finally, the quantification of human lives during wartime also needs to be touched upon. Is it permissible for a commander of troops to send those troops to their certain deaths in order to save a larger number of human lives? In Hollywood films volunteers are solicited who know their chances of survival are negligible. In the legal literature one certainly does find authors who maintain that an order sending soldiers to their deaths is a lawful order in German law under § 11 (1) of the Soldiers Act (*Gesetz über die Rechtsstellung von Soldaten* – SoldatenG) [44]. Finally, the quantification problem is also discussed in the context of the distribution of scarce resources in the health care sector (i.e. medical triage decisions).[45]

IV. Special problems

We still need to discuss whether other factors must be taken into account, when weighing "life against life", in addition to the factor quantity (in symmetrical risk community cases). According to the normative requirements of the German Federal Constitution (*Grundgesetz* – GG), factors such as age, gender, ethnicity, health, etc., are from the outset not considered relevant factors.

---

44 On this discussion, see for example Eser, "Töten im Krieg: Rückfragen an das Staats- und Völkerrecht" in Appel *et al*., (eds.) *Öffentliches Recht im offenen Staat. Festschrift für Rainer Wahl zum 70. Geburtstag*, 2011, p. 665 – 687 (675 *et seq*.); Leisner, Das *Lebensrecht*, 1976, p. 38, who even considers obvious "suicide missions" to be legitimate, provided that many people could be saved.

45 Giesen, *Juristenzeitung* 1990, 929 (941 *et seq*.).

1. The probability of being injured

There is very much to be said for taking into account the factor "probability of being injured". Who should the computer system decide to run over, therefore, if the two seriously injured people on the ground are very unlikely to be killed by the approaching car, but the pedestrian at the roadside with the greatest certainty would be killed, if the vehicle swerved and hit him? Our ethical intuition speaks in favour of taking into account the probability of injury when weighing the interests of the parties involved. The law also requires that it be considered, when § 34 StGB focuses on the "…the degree of … danger facing them …." It seems, however, that we have reached the limit of what can be meaningfully asserted given the present state of our knowledge. In seems very unlikely in the foreseeable future, that it will be possible to accurately quantify the probability of injury in real (i.e. not hypothetical) accident situations. At best it will be possible to make qualitative or comparative statements, i.e. statements such as "almost certain", "very likely", "very unlikely" or statements such as "event A is more likely than event B".

In the absence of "hard" probabilities, it is not possible to formulate clear, unambiguous rules for dealing with relevant conflicting interest scenarios. Given the choice of either (a) the certain (or near certain) killing a person or (b) placing one or two persons into situations where the risk of death is low, a decision in favor of choice (b) would probably be in accordance with the moral intuition of most people. In the final analysis, therefore, the majority of arguments are in favour of including the likelihood of injury into the weighing of interests in the dilemma situations in question, also and especially when lives are being weighed against lives.

2. Self-protection measures

How self-protection measures will be fed into the equation remains to be clarified: Suppose a car is in an emergency situation in which it is impossible to avoid a collision. The victim will be one of two cyclists. Should there be a preference for the car to hit the cyclist wearing a crash hel-

met?[46] This would take into account the fact that this person is better protected against injuries in the event of a collision with the car. On the other hand, it would mean that those road users, who try to take appropriate measures to protect themselves, would be treated less well than those who recklessly refuse to use protective devices like helmets. Should the vehicle be steered to hit the cyclist without a helmet, because he has refused to take appropriate safety precautions? This highlights a fact that has often received little attention in the debate so far: From the perspective of those persons who are directly affected, a system designed to avoid collisions can behave like an attack system[47].

The special problem results from the fact that the necessity of minimizing risks and injuries, if possible, i.e. the principle of the lesser evil, conflicts with aspects of prevention. Strictly speaking, potential damage should be minimized and therefore the cyclist with the crash helmet should be hit by the car. This, however, would provide an incentive not to wear a crash helmet, i.e. refrain from taking protective measures in road traffic, which hardly seems acceptable from the perspective of injury prevention. Based on the humanistic understanding of law expressed here, we would have to insist that operating a motor vehicle in such a way that it would kill or almost certainly kill victims who failed to use protective devices is certainly not permissible. Educating road users to use protective devices such as helmets should certainly not be an issue here. In all other cases, the goal should be to maneuver the vehicle is such a way as to make a collision less likely, disregarding the extent to which the victim is wearing protective gear. This approach, however, is only one of several legal policy options which may appear to be acceptable.

3. Actions and omissions

One issue, which could be very important from the point of view of the criminal law, is the distinction between actions and omissions. Not only do offences of omission, in contrast to offences committed through actions,

---

46 In principle, the same question arises with regard to safely designed and less safely designed cars and their passengers (who, for example, may or may not be wearing their seat belts). Cf. also below section 3.

47 Lin, "Why Ethics Matters for Autonomous Cars" in Maurer *et al*. (eds.): *Autonomes Fahren*, 2015, pp. 69 – 85 (72 *et seq*.).

require that additional criteria be fulfilled for criminal liability to be incurred, but according to prevailing German legal opinion it may be easier in the case of homicide offences committed by omission to avoid liability through the use of legal justifications than is the case for offences committed through actions. In particular, according to prevailing opinion, in cases where there are conflicting duties, the legal interest which the actor subject to the conflicting duties decides to protect, does not need to be "significantly more important" than the legal interested he chooses not to protect. Rather, for the legal justification to apply it is sufficient that two equally important legal interests are at risk, and the actor can only protect one of those interests, so he chooses from the two, and protects that legal interest[48]. Let's look at a hypothetical example: As in our previous case, a vehicle is travelling at high speed toward a situation in which three seriously injured persons A, B and C are lying in the road in its path. It does not swerve to avoid running over the injured people on the road, because if it did so it would collide with and kill D, who is standing at the side of the road. One could argue that A, B, and C's deaths were not caused by an action of the driver, but rather through the omission of the driver, namely his failure to swerve to avoid running them over[49]. This would be a way to interpret the facts in order to "create" a potential offence of omission, in which under certain circumstances a legal justification through conflicting duties might arise.

This argument, however, is not convincing for several reasons: A vehicle that simply travels straight forward and collides with a person, without the driver steering to alter the trajectory of the vehicle, harms the victim (here the person struck by the car) through the action of running him over. If it were otherwise, a large proportion of road traffic offences would be offences of omission rather than offences where the perpetrator performed a positive act. The fact that the car could have swerved to the right or left does not change this conclusion[50]. In addition, it should be borne in mind that cases where a vehicle simply moves "straight forward" are probably more the exception than the rule. It is equally conceivable that the vehicle

---

48 Cf. Neumann in Kindhäuser *et al*., (eds.) *Strafgesetzbuch* (Nomos-Kommentar), 2017, § 34 StGB, paragraph 124 e*t seq*.

49 From a purely logical point of view, of course, this argument would be acceptable.

50 Of course a marksman can intentionally miss his target, by shooting to the right or to the left. That does not mean, however, that intentionally missing the target should be regarded as an omission (not hitting the target).

can only turn to the left (injuring person A there) or to the right (injuring person B there) [51].

Furthermore, it is true that in German criminal proceedings a collision of duties can be used as a legal justification by a (human) actor who might otherwise have incurred criminal liability. However, it is certainly not clear that this legal concept can also simply be applied to the actions or omissions of machines controlled by algorithms! More likely would be an assessment of the situation at issue by a court from the perspective of the victim and his fundamental rights. From the perspective of the targeted (innocent) human collision victim, the "behaviour" of the vehicle would be interpreted as an unlawful infringement of his fundamental rights to life and physical integrity (Article 2 (2)(1) GG). Therefore, in the conflict scenarios sketched out above, neither of the alternatives achieves a satisfactory result.

V. The liability of manufacturers of collision avoidance systems

The questions discussed so far have concerned the assessment of concrete emergency situations. This has to be distinguished from two questions: (1) whether manufacturers can be held liable for collision avoidance systems, if property damage or personal injury occur; (2) whether automatic collision avoidance systems, together with their respective programs, should or should not from the outset be licensed for use on public roads because of the risk of unlawful fatal accidents[52].

1. Exclusion of liability using the concept of "accepted risk"

According to the view expressed here, such systems are permissible and their introduction is necessary and desirable. In order to avoid the risk of civil liability but in particular to avoid the risk of criminal liability, it is

51 For example, at a fork in the road, etc.

52 Rejection of their use on public roads, however, would again have to be justified both morally and legally – a pathway back to the state of innocence, before collision avoidance algorithms were technologically feasible, does not appear to be possible. This demonstrates how our technological capabilities not only extend our actual possibilities, but also create responsibilities.

necessary to do everything possible and reasonable during the programming and installation of computer systems, working at the state of the art of the technology, in order to avoid causing damage. Subsequently, the systems must also be monitored, serviced at regular intervals and, if possible, updated[53]. These requirements follow from the doctrine of accepted risk, by which duty of care requirements are restricted in the case of technologies which are deemed to be fundamentally positive[54]. Just as airbags and seatbelts may be (or even must be[55]) installed and used in motor vehicles although in some cases they can result in personal injury or even death, the installation of automatic collision avoidance systems is not considered to be a breach of duty of care requirements (i.e. negligence) as long as all reasonable technological solutions have been implemented in order to minimize potential injuries. This assertion requires a somewhat more detailed explanation:

Society of the present is marked by the development and the constant introduction of new technologies that are accompanied by new risks. This can be seen in new medicines and in new forms of medical treatment as well as in energy production, food production and road transport[56]. The allocation of liability risks has developed into a core problem for the law of present: "In modern 'risk society', interest in the distribution of material goods is being pushed further and further into the background by the more existential concern of how potential risks, which up to now could never have been imagined in their dimensions and ubiquity, should be allocated[57]."

Not every infringement of a legal interest is a criminal offence. The conscious decision that a risk is an accepted risk may appear sensible if

---

53 Such improvements are likely to be made in the future, largely by installing improved software either in repair workshops or by radio.

54 Kindhäuser, *Strafrecht Allgemeiner Teil*, 2017, § 33 paragraph 26; Kindhäuser, *Strafgesetzbuch. Lehr- und Praxiskommentar*, 2017, § 15 paragraph 58.

55 On the legal duty to wear a seat belt, cf. § 21 a German Highway Code (*Strassenverkehrs-Ordnung* – StVO).

56 For a more detailed treatment from a sociological perspective, cf. Hoyer, *Zeitschrift für die gesamte Strafrechtswissenschaft* 121 (2009), p. 860 *et seq*.

57 Duttge, *Zur Bestimmtheit des Handlungsunwerts bei Fahrlässigkeitsdelikten*, 2001, p. 489. On the concept "risk society" and its reception in the law, cf. Hilgendorf, *Strafrechtliche Produzentenhaftung in der "Risikogesellschaft"*, 1993; Reus, *Das Recht in der Risikogesellschaft, Der Beitrag des Strafrechts zum Schutz vor modernen Produktgefahren*, 2010, both with detailed citations.

the associated positive consequences clearly outweigh the negative consequences. The notion of "accepted risk" suggested here may be found scattered in many disparate areas of the law. Karl Binding, to whom we owe thanks for the first more detailed analysis of this concept, referred 100 years ago to this as "isolated traces of a great legal idea"[58]. In particular, accepted risk was recognized very early in connection with trade and technology. There is a motto associated with the Hansa, a very successful confederation of German market towns and guilds, which controlled the Baltic sea trade in the late middle ages: "*Navigare necesse est, vivere non necesse*"[59], which can be roughly translated as: "That we go to sea is necessary, that we all survive is not".

Binding states the idea in a more general way as follows: "The more indispensable an action is in a legal sense, the greater the risk that it can be done without legal repercussions[60]." The "indispensability" of the action can result from its significance for an actor or his relatives, but also because of the meaning it has "for certain sections of society, or for the legal order and the state[61]." The creation of risks is only permissible, however, as far as is necessary[62]. Jakobs has quite rightly pointed out that the permissibility of a risk is often not simply confirmed through a cost-benefit analysis; rather, besides "accepted risk by risk assessment", there also exists accepted risk by virtue of "historical legitimation"[63]. This leads us to the issue of "social adequacy" as a basis for accepted risk[64].

It follows from what has been said, as Ulrich Weber pointed out, "the legal order takes certain risks, even risks to life and limb are tolerated with eyes wide open. This has been done, for example, as legal approval was

---

58 Binding, *Die Normen und ihre Übertretung, Eine Untersuchung über die rechtmäßige Handlung und die Arten des Delikts*, vol. 4: Die Fahrlässigkeit (negligence), 1919, p. 436. For a thorough discussion of the negligence problem today, cf. Duttge, *op.cit.* 2001 (Fn. 57).

59 Binding, *op.cit.* 1919 (Fn. 58), p. 437, who refers to Rümelin, *Schadensersatz ohne Verschulden*, 1910, p. 26.

60 Binding, *op.cit.* 1919 (Fn. 58), p. 440.

61 *Ibid.* (Fn. 58), p. 440 *et seq*.

62 *Ibid.*, (Fn. 58), p. 442.

63 Jakobs, *Strafrecht Allgemeiner Teil*, 1991, 7/36 with reference to BGHZ 24, 21 (26 *et seq*.).

64 An example of the historically and culturally based differential treatment of social risks, which can be examined from a legal perspective using the concept of social adequacy, is the lawfulness of selling "hard" alcoholic beverages, on the one hand, and the ban on cannabis, on the other.

given to motorized road transport and to the operation of hazardous installations, but only on the condition that the parties observed strict safety precautions. If these rules are complied with... a negligence claim cannot be raised even if a socially damaging consequence is the result … for example, a road user is injured or even killed. [65]"

These considerations can be directly applied to the issues raised here: The installation and operation of automatic collision avoidance systems may not in principle be regarded as negligent, even if it is clear that such systems (statistically with near certainty[66]) will also result in harm to human beings under very unfavorable conditions. Certainly, the prerequisite for this is that the systems are designed in such a way that the extent of possible damage is kept as low as possible. The safety rules to be observed thereby can be explicitly stipulated in technical rules, but they can also result from the analysis and assessment of individual cases[67].

This does not mean that the injury or even killing of an innocent person could be justified by the use of an automatic collision avoidance system (i.e. be lawful). This would be contradicted by Art. 2 (2)(1) GG which places human life under special protection. From the fact that reliance and use of automatic collision avoidance systems is not adjudged to be negligent, it certainly does not follow that if such a system were to kill a human being in an extreme case – one might even say a "misadventure" – this killing would be lawful. The person concerned does not have to tolerate his life being put at risk, which ought to go without saying, but can try to avoid the danger or defend himself.[68]

---

65 Baumann, Weber & Mitsch, *Strafrecht Allgemeiner Teil*, 11th ed., 2003, § 22 paragraph 14. On this subject, see also Duttge*, op.cit.* 2001 (Fn. 57), p. 104 *et seq*.

66 Nevertheless, it would not be convincing to assume that manufacturers or programmers intend to cause injuries, since in spite of the fact that such damage is statistically almost certain to take place, it cannot be known in advance, when, at which place, and caused by whom, such accidents will occur.

67 In general, compliance with technological rules is not the same as fulfilling the duty of care required in road transport, since the duty of care required in individual cases may go beyond what is necessary to comply with relevant technological rules (which may not be appropriate or no longer appropriate). Compliance with technological rules is, in any event, an indication that the necessary duty of care has been fulfilled. For additional detail, cf. Duttge in *Münchener Kommentar zum StGB*, 2017, § 15 StGB, paragraph 138, which includes further citations.

68 It should be noted that reliance on self-defence under § 32 StGB should be ruled out in the absence of a physical attack. There remains, however, recourse to the defence of necessity under § 34 StGB.

The installation and use of powerful motors, the use of a metal body panels, and the authorization of motorized road transport as such[69], create risks that can in individual cases result in the deaths of human beings. Nevertheless, the companies that sell powerful car motors and steel car body panels, are no more negligent than the state that permits motorized road transport because the benefits that accrue from these actions more than offset the damage they cause. It is obvious that the killing of human beings through road transport is per se not justified. It would be erroneous to derive an obligation to tolerate individual cases in which risk threatens to be realized (i.e. injury incurred) from the social acceptance of the creation of risk.

2. Counterarguments

Engländer has expressed opposition to the limitation of liability by means of the concept of "accepted risk" in the context of automatic collision avoidance systems in road transport[70]. His arguments, however, do not stand up to critical analysis.

According to Engländer, the two characteristic features of accepted risk are, firstly, "as an exception, the general usefulness of an activity which may cause harm", and, secondly, a "lack of power to avoid causing harm on the part of an actor, for which he himself bears no responsibility, meaning the inability to prevent the result in individual cases (to the extent that the actor is not prepared to completely renounce engaging in the respective activity)" [71]. Engländer regards accepted risk as a ground for excluding objective attribution, and not, as I have suggested,[72] as a means of limiting negligence claims, which accords with prevailing opinion. Perhaps, this is one reason why Engländer confounds "accepted risk" with respect to the responsibility of vehicle users, with the responsibilities of manufac-

69 Cf. the previously cited statement of Ulrich Weber in Baumann, Weber & Mitsch, *op.cit.* 2003, § 22 paragraph 14. (see above, Fn. 65).

70 Engländer, *Zeitschrift für Internationale Strafrechtsdogmatik* 2016, 608 (612).

71 *Ibid.*

72 Expert testimony before the Committee on Economic Affairs and the Media, Infrastructure, Construction and Transport, Energy and Technology of the Bavarian State Parliament, 17th electoral period, 38th meeting, 19.10.2015, p. 50 (available at https://www.bayern.landtag.de).

turers for the programming and marketing of their collision avoidance assistants.

Engländer deals firstly with the possibility of vehicle users incurring criminal liability[73].

As a possible *actus reus* which could incur criminal liability, he correctly points to "putting the appropriately programmed vehicle into motion"[74]. As a possible element of an offence, here the criminal result, he refers to the "death, bodily harm, damage to property of another road user"[75]. Amazingly, however, at this point Engländer does not discuss issues of intent or negligence, but focuses solely on the concept of accepted risk. If accepted risk is used as an instrument for limiting negligence claims, this question does not arise because the user of a vehicle with a properly functioning collision avoidance system is not negligent when a correspondingly programmed vehicle is used. A user cannot predict the occurrence of a concrete accident situation in which the collision avoidance system would intervene. Thus it can be seen that a key prerequisite to substantiate a negligence claim is missing, so that the question of restricting the duty of care required by law by means of the concept of accepted risk does not arise.

Rather confusingly, Engländer then explains that the vehicle user (!) possesses the "power to avoid causing the harm" he postulated, since the occurrence of the factual result could "very simply" have been avoided by programming the collision avoidance system differently. That is true, but only as regards the manufacturer or programmer, and certainly not the vehicle user. The vehicle user could only avoid the intervention of the collision avoidance system by not starting up the car, which means that he has to renounce the activity for which he is accused in the first place.

The change of perspective, which is not explained at all, makes it difficult to understand Engländer's argumentation, especially since he later affirms the concept of accepted risk, albeit in favour of manufacturers, under certain circumstances[76]! In this case, the issue of "power to avoid causing harm" by reprogramming the system (which only manufacturers or their programmers are able to do) is apparently are no longer important.

A manufacturer who programs his automatic collision avoidance system according to the rules developed in the first part of this paper, may, in

---

73 Engländer, *op.cit.* 2016, 608 (611 *et seq*.).
74 *Ibid*., p. 611.
75 *Ibid*.
76 *Ibid*., p. 617.

our view, rely on the concept of accepted risk. From a legal point of view, the development and installation of such systems into motor vehicles do not represent a misdeed, even if a (subsequent) death caused by such a system constitutes a wrong[77]. The same (approach) applies here as it does to the use of seat belts and automatically opening airbag systems, which similarly in almost all cases protect their users from harm, but do in rare cases cause deaths, without the manufacturers of such systems incurring negligence liability as long as the systems have been designed as safely as possible, given the current state of the art of the technology.

3. Passenger protection

The question remains whether the manufacturer, in the present context, in ensuring the safety his vehicles (and especially their occupants) is subject to new ethical or legal restrictions. If one applies the rules developed above, this is not the case: vehicle occupants are (of course) not obliged to acquiesce in being injured or killed.

Collision avoidance assistants, which are installed into motor vehicles, must be programmed in such a way that vehicle occupants are protected under all circumstances. Only the case of the symmetrical risk community is problematic, i.e. where two (or more) persons or groups of persons face the same risk. In our view, the principle of the lesser evil should be applied in such cases.

This can be visualized using two examples. A vehicle is travelling toward a number of persons lying on the road. It can neither swerve nor brake safely to avoid killing those persons. According to the view presented here, the driver is not under an ethical or legal duty to drive in such a way as to destroy his own vehicle (for example, by swerving so as to collide with a concrete pillar or some other self-destructive manoeuver), even if the number of people saved would exceed the number sacrificed. This is not a case of a symmetric risk community.[78]

The situation is completely different when a car at high speed is approaching a broken down truck carrying explosives, which is blocking the road. The explosion caused by a collision would not only kill the three oc-

77 See Weber citation above (Fn. 65).
78 See above, p. 71.

cupants of the truck but also the driver of a vehicle approaching in the opposite direction. In such cases, where a symmetric risk community exists, according to the view presented here, the vehicle which is about to collide with the truck must in principle attempt to avoid the collision by swerving, even if this would seriously endanger the life of the occupants of that vehicle[79].

Such cases should, of course, only occur in theory. Manufacturers are responsible for ensuring the lives and the physical integrity of the occupants of their vehicles by installing high performance safety systems. The solution presented here is simply a further incentive for them to continually optimize passenger safety. In addition, it would be as unreasonable for car manufacturers to be under a legal duty to install "self-destruction mechanisms" in their vehicle as it would be to legally require buyers to use such vehicles[80]. Manufacturers are under no legal duty to produce cars which put their "own" passengers into significant danger or even sacrifice the lives of those passengers, but rather motor vehicles should and must be made to be as safe as possible, even if complete safety can never to be achieved.

4. What risks should be considered "accepted" risks?

This leads to the question as to which risks a society regards as "acceptable" and therefore wishes to classify as "accepted" risks. In a democratic state, the answer requires a process of social debate and "negotiation". Essential variables for answering this question should include objective and verifiable criteria such as levels of possible damage, probability of occurrence, possibilities for prevention, and the issue of whether or not damage is irreversible. In social reality, however, the acceptance of technological risk is shaped by historical contingencies and often hardly reconstructible prejudices and habits. Even risk perception varies considerably from person to person[81]. Lawyers are part of society and convey social risk aware-

---

79 See above, p. 84.

80 On the principle of reasonableness, see Hilgendorf & Valerius, *Strafrecht Allgemeiner Teil*, 2015, § 11 paragraph 90: An action is unreasonable if, as a result, one's own legitimate interests are harmed to a considerable extent.

81 One example from the area of anti-drug policy are the different perceptions of risks associated with alcohol and cannabis. For further detail on the risk debate, cf.

ness into the judicial decision making process (and under certain circumstances into the legislative process). It is the task of a rational analysis of the consequences of technological development[82], based on empirical research, to accompany and influence the debate on which risks should be considered "accepted risks".

It could be feasible to introduce a kind of "algorithm seal of technical approval" for automatic collision avoidance systems (and perhaps for other algorithms that have to make particularly risky decisions), i.e. a special approval procedure, which would be required before a system could be put onto the market. The competent authority for the implementation of such a procedure should be a state authority whose work is subject to safeguards generally accepted in states under the rule of law. One could also imagine certification procedures. In this way it should be possible to control and "fence in", via norms, technological development in the area of algorithms so as to preserve the humanistic imperative of always accepting the fundamentally free individual, with his special dignity as a human being, as the guiding value of our law and jurisprudence on that law[83].

Although, according to the view represented here, the installation of automatic collision avoidance systems is not to be adjudged negligent because the risks created by them in a very small number of cases are more than outweighed by the significant utility they provide in the overwhelming majority of cases, there is still one point which needs to be emphasized. This was looked at by Binding[84]: risk creation is only permitted to the extent that it is *necessary* to achieve the intended benefits for society. What we are dealing with here is a criterion that can be empirically tested. Every risk creation, which goes beyond what is strictly necessary, is reprehensible. This means that new technological systems must be designed in such a way as to minimize the risks created by them. We will once again be able to speak of degrees of wrong and of the duty to reduce the wrong

---

Fischhoff & Kadvany, *Risk, A Very Short Introduction*, 2011; Renn & Zwick, *Risiko- und Technikakzeptanz*, 1997; for a recent contribution, cf. Renn, *Das Risikoparadox. Warum wir uns vor dem Falschen fürchten*, 2014.

82 Grunwald, *Technikfolgenabschätzung. Eine Einführung*, 2nd ed. 2010; cf. also Grunwald, *Technik und Politikberatung. Philosophische Perspektiven*, 2008.

83 Cf. above p. 63 et seq.

84 Cf. above Fn. 58.

to a minimum. In doing that, of course, the general legal principle of reasonableness must be observed[85].

The results found for collision avoidance systems can be extended to all technological (and non-technological) products: their development and their use are permitted, even if their use in individual cases can lead to unintended damage, provided the risks arising from them can be considered acceptable[86]. It does not matter whether one treats accepted risk as a separate concept within the legal doctrine[87] of negligence or merely as the *other side* of the duty of care obligation[88]. It is an important principle of modern product liability law or producer liability law[89].

VI. Closing remarks

The results can be summarized in the following theses:

1. The transfer of human decision making to algorithm-driven technological systems forces us to make processes explicit, which had previously been done without reflection. That means raising them to the level of con-

---

85 See above Fn. 80. This means among other things, that manufacturers are not obliged to incur expenditures that could jeopardize their economic competitiveness or even their existence. On the other hand, the state is obliged to ensure adequate protection of its citizens, even in the face of technological developments (above Fn. 36), p. 35.

86 Vogel in *Strafgesetzbuch Leipziger Kommentar*, 2012, § 15 StGB, paragraph 279.

87 For example, according to Lenckner & Sternberg-Lieben in Schönke & Schröder, *op.cit.* 2014 Vor §§ 32 *et seq*. StGB, paragraph 107 b.

88 Kindhäuser wrote in "Zum sog. 'unerlaubten' Risiko", in Bloy *et al.* (eds), *Gerechte Strafe und Legitimes Strafrecht: Festschrift für Manfred Maiwald zum 75. Geburtstag*, 2010, p. 397 (404): "Whoever engages in dangerous acts which are accepted, does not violate his duty of care. And vice versa: Anyone violates his duty of care, engages in dangerous acts which are not accepted." Cf. also Duttge in *Münchener Kommentar zum StGB*, 2017, § 15 StGB, paragraph 139. This language usage corresponds to everyday (German) language. In this context, however, the concept of accepted risk is clearly understood in a much wider sense than in the above text, where its use is restricted to the development and marketing of hazardous products.

89 Cf. also § 3 Product Liability Act (*Produkthaftungsgesetz* – ProdukthaftG), according to which a product is defective "when it does not provide the safety which one is entitled to expect, taking all circumstances into account, in particular its presentation, the use to which it could reasonably be expected that it would be put, the time when it was put into circulation." Absolute security cannot be expected.

sciousness and subjecting them to analysis. One could almost speak of a *compelling need to explicate* going hand in hand with the "algorithimization" of the world we live and work in. The conflict dealt with here is, in this respect, only one of many decision making situations which must be rethought in ethical and legal terms.

2. In modern road transport, the *principle of the lesser evil* applies in the event of an emergency situation. This is a general principle of our law. It follows, inter alia, that the protection of life and limb must always take precedence over the protection of property.

3. The principle of the lesser evil becomes problematic when serious personal injuries have to be weighed against one another. This is especially true in the context of life threatening situations.

4. The killing of an innocent human being by an automatic collision avoidance system cannot be justified by saving a greater number of lives. Based on legal-ethical considerations, which are ultimately rooted in legal humanism, the individual human being is the maximum value in our legal order. In principle, he must not be compelled to sacrifice his own central ("essential") legal interests for the benefit of others.

5. Qualitative characteristics such as age, gender or ethnic origin may not play a role in the assessment of emergency situations. In contrast, the probability of violations of legal interests should be taken into account in computer-controlled decision-making processes.

6. When weighing-up road traffic collisions, considerable difficulties are posed by considerations of the safety precautions of respective road users. As a matter of principle, causing death and serious personal injury must if possible be avoided. Personal issues and characteristics may not play a role in accident prevention and avoidance.

7. The thesis that lives cannot be quantified, if taken literally, is incorrect. Such quantifications are, in certain cases, even morally and legally necessary, for example, when applying the proportionality principle.

8. In emergency situations, in which the lives of several people are equally threatened (symmetrical risk community), an assessment of degrees of wrong should be undertaken: The killing of every innocent human being is legally wrong. Nevertheless, the number of innocent victims should be kept as low as possible. This assumes both the quantification of potential victims, as well as respect for the principle of the lesser evil.

9. In contrast, in cases where a symmetrical risk community is not present, i.e. where all persons involved do not from the outset face equal or at least comparable life-threatening risks, those persons who are not at

risk of serious injury or death should not be put at risk. The prohibition on "redistribution of chances of survival" follows from the same humanistic principles discussed previously in the context of balancing lives (cf. 4 above).

10. The development and use of automatic collision avoidance assistants cannot be regarded as negligent, because, although they create certain risks, these risks are more than offset by their practical benefits (so-called accepted risk). Rather they operate like other technological systems both in and outside the context of road transport: If they provide major social benefits, for example, by significantly increasing the safety of road transport, the development and use of such systems are permissible, even if the systems can cause damage in individual cases that cannot per se be justified.

11. Automatic collision avoidance systems, however, must be designed in such a way that the damage they cause is reduced to the absolute minimum. Thus the principle of the lesser evil applies here, too. The issue of reasonableness is important when considering ways to optimize safety. Manufacturers should and must make their vehicles as safe as possible.

12. The concept of accepted risk can be applied in the research, development, and marketing of all sorts of goods, including but not limited to technology based products, in addition to automatic collision avoidance systems. It is a general principle of modern product liability law and producer liability law, which is likely to play a key role in the future clarification of the legal issue of liability for damage caused by automatic systems.

Criminalizing attacks against information systems in the EU and the impact of the European legal instruments on the Greek legal order*

Maria Kaiafa-Gbandi#

1. Introduction

Admittedly, information technology has radically and irrevocably changed modern societies. In technologically advanced countries, information systems have infiltrated virtually every sector of social life to such an extent as to redefine both State and individual activities. Government, national defense, communications, transportation, health systems, education, and entertainment are but a few among many fields administered by the so-called "information society".[1] Personal computers on their part have affected the everyday lives of all citizens, as evidenced for instance in the widespread use of e-mail and the dissemination of information on the worldwide web.

The unprecedented economic and social changes brought about by these developments have rendered information systems –as well as the data circulated therein- fundamental interests worthy of protection. This only makes sense, given the implications of the potential abuse of an information system: a mere click of the mouse can cause massive power outages, cancel out copious scientific efforts, and even bring about nuclear holocaust through the breach of information systems running nuclear reactors.

---

* The present article is a redacted and updated version of a paper published in the European Journal of Crime, Criminal Law and Criminal Justice 2011/1.

Prof. Dr. Maria Kaiafa-Gbandi, Law Faculty, Aristotle University Thessaloniki.

1 See indicatively *St. Furnell* (2012), Cybercrime – Vandalizing the information society, 1 ff., *M. Gercke,* Herausforderungen bei der Bekämpfung der Internetkriminalität, in *M. Gercke*, and *Ph. Brunst* (2017), Praxishandbuch Internetstrafrecht, 7-9; *cf*. the Explanatory Report to the Cybercrime Convention by the Council of Europe, paras. 1-6.

Without a doubt, this dark side of the use of information systems might be the single most important challenge information society has to face.[2]

It soon became clear that the applications of information technology had to be accompanied by pertinent regulation.[3] As far back as the '80 s, a number of legal orders recognized information systems as fundamental interests worthy of protection, and adopted criminal law rules to proscribe their breach.[4]

The rapid growth of the worldwide web has made it palpable that the impact of criminal conduct against information systems is unrestrained by national or geographic boundaries, hence ringing an alarm for the international community.[5] Considering that malicious viruses can be unleashed from anywhere in the world, no viable solution can be achieved in the absence of international cooperation[6]. This is especially true of a supranational organization like the E.U., which aspires to establish a common area of freedom, security and justice (articles 67 and 82 *et seq*. TFEU) also by addressing serious crime with a cross-border dimension (article 83, par. 1

---

2 *Cf*. the analysis of *M. Sieber*, Computer crimes, cyber-terrorism, child pornography and financial crimes, in Spinellis D. (ed.) (2004), Computer crimes, cyber-terrorism, child pornography and financial crimes, 14 ff.; *P. Jougleux, L. Mitrou,* and *T. Synodinou*, Criminalization of attacks against information systems, in I. Iglezakis (ed.) (2016), The Legal Regulation of Cyber Attacks, 34; *T. Politis, Ph. Kozyris,* and *I. Iglezakis* (eds.) (2009), Socioeconomic and Legal Implications of Electronic Intrusion; *J. Martin-Ramirez* (2017), Cyberspace, 141ff. On the socioeconomic background of cybercrime see indicatively *M. Karyda*, The socioeconomic background of cybercrime, in D. Politis, Ph. Kozyris and I. Igrlezakis (eds.) (2009), Socioeconomic and Legal Implications of Electronic Intrusion, 1ff.

3 For a survey of pertinent developments through time see, inter alia, *M. Kaiafa-Gbandi* (2007), Criminal law and abuses of information technologies [in Greek], Arm, 1059, with further citations.

4 Articles 370ter and 370^{quater} were introduced into the Greek Criminal Code in 1988, while German law had incorporated similar provisions by virtue of a statute dated 15.5.1986 (Zweites Gesetz zur Bekämpfung der Wirtschaftskriminalität – 2. WiKG). For an interesting recent comparative study on criminalizing cyber aiding see *T. Zhang* (2017), A comparative study on sanction system of cyber aider from perspectives of German and Chinese criminal law, Computer Law and Security Review 33, 98ff.

5 See the Explanatory Report to the Cybercrime Convention, paras. 5-6, and *M. Gercke* (2010), Impact of the Lisbon Treaty on Fighting Cybercrime in the EU, CRi, 75.

6 *K.-L. Hui, S.-H. Kim,* and *Q.–H. Wang* (2017), Cybercrime Deterrence and International Legislation: Evidence from Distributed Denial of Service Attacks, MIS Quarterly (41:2), 497ff.

TFEU),[7] including cybercrime. Besides, the approximation of domestic criminal law in this field is the first step towards achieving harmonized approaches in the field of procedural law, as well as facilitating judicial cooperation.

It becomes evident that, when it comes to the criminal law protection of information systems, European and international initiatives become central, as they largely determine the position of national legislatures.

2. *The European and international institutional framework concerning attacks against information systems*

2.1. A comparative survey of a complex framework

The Council of Europe Convention on Cybercrime holds a central position on the international plane.[8] The said convention requires State-parties to proscribe not only *stricto sensu* computer crimes[9] –i.e. those posing a direct threat to information systems and digital data- but also other types of crime perpetrated by means of a computer (such as computer fraud), including content-related crime (such as child pornography). Despite its flaws,[10] the Convention on Cybercrime has thus emerged as the most com-

---

7 On the pertinent competence of the E.U. see indicatively *M. Kaiafa-Gbandi* (2011), European criminal law and the Lisbon Treaty [in Greek], 29 ff.

8 See CETS No. 185, Budapest, 23.XI.2001, in force 1.7.2004.

9 On the distinction between genuine and non-genuine computer crimes see *Kaiafa-Gbandi* (2007), Arm, 1062. On the distinctions drawn in the field of computer crime in general see *D. Kioupes*, Combating computer crime in the European Union [in Greek], in Piraeus Bar Association – Hellenic Criminal Bar Association – Center of International, European and Economic Law, Contemporary developments in European Economic Criminal Law (2010), 191 ff.

10 With respect to matters pertaining to fundamental rights, personal data, and procedural rights see, inter alia, *P. Breyer* (2001), Die Cyber-Crime-Konvention des Europarats, DuD, 600, *A. Dix* (2001), Regelungsdefizite der Cyber-Crime-Konvention und der E-TKÜV, DuD, 588 ff., *D. Kugelmann* (2001), Die Cyber-Crime Konvention des Europarates, DuD, 222 ff., *id.* (2002), Völkerrechtliche Mindeststandards für die Strafverfolgung im Cyberspace-Die Cyber-crime Konvention des Europarates, TMR, 21 ff., *Br. Valerius* (2004), Der Weg zu einem sicheren Internet?, K&R, 517-518; with respect to substantive criminal law see *I. Carr*, and *K. Williams* (2002), Draft Cyber-Crime Convention, Criminalization and the Council of Europe (Draft) Convention on Cyber-Crime, Computer Law & Security Report, 83 ff.

prehensive instrument in the international fight against cybercrime,[11] owing in part to its provisions on procedure and judicial cooperation.

Although the E.U. itself is not a signatory party to the Convention, all of its member States have signed it, while most of them have already ratified it. In fact, the European Commission "actively encouraged" the member States to ratify the Convention as soon as possible,[12] despite the adoption of a framework-decision on attacks against information systems in 2005,[13] which has been replaced by a pertinent directive, owing to the novel institutional framework introduced by the Lisbon Treaty.[14]

States which happen to be members of both the Council Europe and the E.U. are therefore faced with the dual challenge of harmonizing their domestic law to the Convention on Cybercrime and the directive alike.[15] Yet the E.U. might not realistically dispense with the need of proposing a legal instrument of its own by merely becoming a party to the Council of Europe Convention. This is because a supranational organization such as the E.U. is in a much better position to bind its member States to follow its decisions; in addition, it can expand the proscribed types of conduct, ad-

11 See, e.g., *P. Csonka* (2000), The draft Council of Europe Convention on Cyber-Crime: A Response to the Challenge of Crime in the Age of the Internet?, Computer Law & Security Report, 329, *M. Gercke* (2004), Die Cybercrime-Konvention des Europarates, CR, 782 ff., esp. at 786, *id.* (2004), Analyse des Umsetzungsbedarfs der Cybercrime-Konvention, MMR, 728, *id.* (2006), The Slow Wake of A Global Approach Against Cybercrime – The potential of the Council of Europe Convention on Cybercrime as international model law, CRi, 144-145, *H. Kaspersen* (2001), Council of Europe's Cybercrime Convention, in ERA, Cybercrime: Developing the legal Framework in Europe-Documentation, London, 11-12.11.2010.

12 See Directive 2013/40/EU preamble sect. 15.

13 2005/222/JHA, 24.2.2005, OJ L 69 of 16.3.2005, 68.

14 See Proposal for a Directive of the European Parliament and of the Council on Attacks against Information Systems, replacing Council Framework Decision 2005/222/JHA in COM (2010) 517 final, of 30.9.2010; *cf*. the Presidency's proposal to the Council 8795/11, DROIPEN 27-TELECOM 43- CODEC 609, of 8.4.2011 and Directive 2013/40/EU; also see *D. Brodowski* (2010), Strafrechtsrelevante Entwicklungen in der Europäischen Union-ein Überblick, ZIS, 753-754 and *Ph. Jougleux, L. Mitrou and T. Synodinou*, Criminalization of Attacks against Information Systems, in I. Iglezakis (ed.) (2016), The Legal Regulation of Cyber Attacks, 25ff..

15 *Cf. F. Sanchez-Hermosilla* (2003), Neues Strafrecht für den Kampf gegen Computerkriminalität- Konvention des Europarates und neuer Rahmenbeschluss der Europäischen Union im Vergleich mit dem deutschen Strafrecht, CR, 774 ff.

just the applicable rules to correspond to ever-evolving needs, and determine not only "what" will be punished but also "how" it will be punished.[16] In doing so, it is to keep an eye open for initiatives by the Council of Europe affecting its member States, so that it may align its actions accordingly.

It follows that States like Greece or Germany, i.e. EU Member States, had better subscribe to a comparative approach, starting from the E.U. directive, while keeping in mind the Council of Europe Convention on Cybercrime.

2.2. The reasons for the E.U. directive and the core questions arising in a comparative context

On September 30, 2010, the Commission came up with a proposed directive on attacks against information systems, aiming at replacing the existing framework-decision 2005/222/JHA.[17] Less than one year before, the Lisbon Treaty had come into effect, by virtue of which the E.U. was granted the authority to establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension based on the principle of majority (article 83, par. 1 TFEU).[18]

The declared reason for this initiative was "emerging threats highlighted by recent attacks across Europe since the adoption of the framework decision, in particular the emergence of large-scale simultaneous attacks against information systems and the increased criminal use of the so-

16 On the competence of the E.U. in the field of substantive criminal law after the Lisbon Treaty see *Kaiafa-Gbandi* (2011), European criminal law and the Lisbon Treaty [in Greek], 28-34.

17 See pertinently *S. Bier* (2005), Kampf gegen die Cyberkriminalität, Der Rahmenbeschluss 2005/222/JI des Rates der EU über Angriffe auf Informationssysteme, DuD, 473 ff.

18 It is noteworthy that the TFEU (article 83, par. 1) explicitly enumerates computer crime among types of crime with a cross-border dimension triggering the E.U.'s competence to establish minimum rules in the field of criminal law. In fact, the term 'computer crime' was deliberately chosen to cover a broder array of cases compared to 'cybercrime' as provided in the Council of Europe Convention: see *Gercke* (2010), CRi, 79.

called 'botnets'".[19] These factors, which emerged after the framework decision had been adopted, prompted the Commission to seek more effective ways of addressing the threat. According to the Commission, "the main cause of cybercrime is the vulnerability of information systems resulting from a variety of factors, while insufficient response by law enforcement mechanisms contributes to the prevalence of these phenomena, and exacerbates the difficulties, as certain types of offences go beyond national borders. Furthermore, variations in national criminal law and procedure may give rise to differences in investigation and prosecution, leading to differences in how these crimes are dealt with. Developments in information technology have exacerbated these problems by making it easier to produce and distribute tools ('malware' and 'botnets'), while offering offenders anonymity and dispersing responsibility across jurisdictions."[20] In this new environment, the Commission has attempted to formulate its proposal,[21] taking into account novel forms of cybercrime, including the use of botnets.[22]

The EU directive explicitly relies on the Council of Europe Convention on Cybercrime and it poses three core questions:

(i) How are criminal law provisions to be delineated to address attacks against information systems?
(ii) What is the relationship between the E.U. directive with the pertinent provisions of the Council of Europe Convention on Cybercrime?

---

19 COM (2010) 517 final, 30.9.2010, 2 and Directive 2013/40/EY preamble sect. 5.

20 *Ibid*., at 3.

21 The need for further measures to combat cybercrime has been highlighted by the Commission in the context of the Stockholm Program (and the pertinent action plan); moreover, the digital agenda drafted in the framework of the "Europe 2020" strategy features new forms of crime –and especially cybercrime- as its first item: see COM (2010) 517 final, 30.9.2010, 4. *Cf*. the opinion of Europol member *N. Dileone*, Cybercrime: Developing the legal framework in Europe, in ERA, Cybercrime: Developing the legal framework in Europe – Documentation, London, 11-12.11.2010, and Commissioner *R. Jansky*, EU legislative and non-legislative instruments against cybercrime, in ERA, Cybercrime: Developing the legal framework in Europe – Documentation, London, 11-12.11.2010.

22 On 'botnets' and the dangers inherent in their use see COM (2010) 517 final, 30.9.2010, 3-4.

(iii) Last but not least, what is the underlying foundation of the choices made in this directive, placed in the context of fundamental principles of European criminal law after the Lisbon Treaty?[23]

2.3. A comparative survey of the criminal law rules on attacks against information systems on a European and international level

2.3.1. An initial approach

As already noted, the EU proceeded to a new directive on attacks against information systems, because it deemed the existing framework decision deficient in terms of addressing the full array of cybercrime, safeguarding against large-scale attacks, and providing for adequate sanctions.[24]

Specifically, the directive requires member States to proscribe two additional types of conduct (in line with the Council of Europe Convention), namely the illegal interception of computer data (article 6) and the production, sale etc. of tools used for committing computer offenses (article 7), in addition to the ones already covered (illegal access to information systems – article 3; illegal system interference – article 4; illegal data interference – article 5). Even with regard to conduct already covered by the replaced framework decision, the directive introduces changes pertaining to incitement, aiding and abetting, attempt (article 8), and especially applicable penalties (articles 9 to 12), including aggravating circumstances (article 9 paras 3 and 4). In terms of procedural matters, the directive introduces provisions on jurisdiction (article 12), as well as exchange of information (article 13), requiring member States to ensure that they have procedures in place so that in urgent requests they can indicate within a maximum of 8 hours at least whether the request for help will be answered. At the same time, the directive requires the establishment of a system for the recording, production and provision of statistical data on the offences referred to in articles 3 to 7 (article 14).

---

23 See pertinently *European Criminal Policy Initiative* (ECPI) (2009), A Manifesto on European Criminal Policy, ZIS, 707 ff.; *cf. Chr. Mylonopoulos* (2011), European Criminal Law after the Lisbon Treaty: The legitimization of European Criminal Law and the importance of criminal law doctrine for its shaping, PChr, 86-87.

24 See COM (2010) 517 final, 30.9.2010, 4.

2.3.2. Proscribed types of conduct

Starting with the types of conduct already provided for in the replaced framework decision, it is to be noted that the directive does not expand the ambit of *illegal access to information systems*, as contrary to the relevant Commission's proposal it recognizes each member State's discretion to confine the proscribed conduct to situations where the offense is committed by infringing a security measure.

The directive goes even further than the Council of Europe Convention, which allowed some margin of discretion to member States under article 2, just like the framework decision. In fact, the Convention not only allows States to exclude offenses not committed by infringing security measures or are unrelated to a computer system that is connected to another computer system, but also permits them to narrow criminal liability through the introduction of subjective elements, such as requiring 'dishonest intent'. In reality, the Council of Europe was attempting to exclude conduct which does not pose any threat whatsoever to information systems, especially when it might reveal some of their weaknesses.[25] Hence, it left State parties the choice of determining for themselves whether to subscribe to a broad or narrow version of criminalization of cybercrime.

One might counter argue that the same discretion is reserved for member States under the directive, which requires criminalization in "cases which are not minor".[26] However, this would be an erroneous assumption. Indeed, the same clause is to be found in the replaced framework decision 2005/222/JHA *alongside* a provision permitting member States to only criminalize conduct infringing a security measure, indicating that these are two distinct limitations. Notwithstanding the inherent ambiguity of the notion of "minor cases", it cannot be argued that every conduct not infringing a security measure is a minor one. Therefore, the possible exclusion of minor cases under the proposed directive cannot be said to fully coincide with the ambit of either the Council of Europe Convention or the replaced framework decision.

Besides, allowing States to introduce certain limitations is also in line with the requirement that criminal law be used as a last resort (*ultima ratio*

25 See the Explanatory Report by the Council of Europe, para. 49.
26 See, along these lines, *Brodowski* (2010), ZIS, 753.

principle),[27] particularly in view of the fact that efficient security measures could protect information systems much more efficiently than unrestrained criminalization.[28] In that sense, one can only applaud the directive having introduced the infringement of security measures as a requirement for the affirmation of illegal access to information systems.[29]

On the other hand, the provisions concerning illegal system interference (article 4) and illegal data interference (article 5) remain unchanged compared to the replaced framework decision. In addition, only minor discrepancies are traceable with the Council of Europe Convention in this respect. As regards *illegal system interference*, the directive calls for its criminalization "at least for cases which are not minor". That same limitation –albeit not contained in so many words under article 5 of the Council of Europe Convention- derives from the proscribed act itself, which alludes to "serious hindering" of a computer system, thereby rendering the exclusion of minor cases redundant. As regards *illegal data interference*, article 5 of the directive is not identical with article 4 of the Council of Europe Convention. The latter explicitly recognizes that State-parties may reserve the right to require that the conduct result in *serious harm*, while the directive again allows only for the exclusion of *minor* cases. In other words, the Council of Europe Convention also allows for the exclusion of offenses of *average* gravity, thus conceding that other measures, such as administrative sanctions, might be enough to address these.[30] Such choice shows respect for the *ultima ratio* principle,[31] entrusting the pertinent decision with each State-party.

With respect to the novel provision concerning *illegal interception of non-public transmissions of computer data by technical means* (appearing for the first time in an E.U. legal instrument), the Council of Europe Convention allows States to only criminalize conduct committed with dishonest intent or in relation to a computer system that is connected to another

---

27 On the application of this principle in European Criminal Law see *ECPI* (2010), at 707.

28 *Cf.* the Explanatory Report by the Council of Europe, para. 45; also see *Carr*, and *Williams* (2002), Computer Law and Security Report, 84.

29 See Art. 3 of the Directive 2013/40/EU.

30 See pertinently the Explanatory Report by the Council of Europe, paras. 64, 69.

31 For the importance of this principle on a European level see *M. Kaiafa-Gbandi* (2010), The importance of core principles of substantive criminal law for a European criminal policy respecting fundamental rights and the rule of law [in Greek], NoV, 2186 ff.

computer system. In contrast, the E.U. has left no such leeway, the only potential limitation emanating from article's 6 possibility to exclude minor cases. Aside from this deficiency, the directive does not even attempt to delimit the notion of 'interception', thus creating some ambiguity. Likewise, the Council of Europe Convention contains no definition of 'interception' either. That being noted, it should be emphasized that the institutional framework introduced under the Lisbon Treaty authorizes the E.U. to establish *minimum* rules concerning the definition of offenses, which inherently calls for unambiguous provisions, permitting an accurate transposition into domestic law.[32] Besides, a mere look at the explanatory report to the Convention on Cybercrime suffices to demonstrate the need for a comprehensive definition, as the Council of Europe interprets it so as to include, among other things, the monitoring or surveillance of the *content* of communications.[33]

The provision of the directive which marks an overly expansive tendency in the E.U. context is however article 7, requiring member States to criminalize "the production, sale, procurement for use, import, possession, distribution or otherwise making available of *a computer program, designed or adapted primarily for the purpose of committing any of the offences referred to in articles 3 to 6 or a computer password, access code, or similar data by which the whole or any part of an information system is capable of being accessed*". There are two notable differences between this provision and the corresponding article 6 of the Council of Europe Convention.

The first difference is article 6, par. 2 of the Council of Europe Convention, which provides that the provision of paragraph 1 shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to therein is for the purpose of authorized testing or protection of a computer system. One might contend that such exception is superfluous, as the requisite intent of the offense could *per se* preclude conduct carried out for an authorized testing or protection of a computer system. However, given the fact that the proscribed conduct lies distant from

32 See *Kaiafa-Gbandi* (2010), NoV, 2196 ff.

33 See the Explanatory Report by the Council of Europe, para. 53. According to Kioupes [Combating computer crime in the European Union, *op. cit*., at 195], the interception of transmitted data constitutes a breach of what he terms as the victim's "digital domestic peace".

any actual harm to computer systems or data, the above clarification can only be regarded as a positive addition. Besides, article 6, par. 1 of the Cybercrime Convention allows State-parties to require by law a minimum number of tools in order for criminal liability to attach to their possession, a circumstance that is absent from the text of the directive.

Secondly, State-parties to the Council of Europe Convention are free to exclude certain types of conduct from criminalization under article 6, par. 1, provided that their reservations do not concern the sale, distribution or otherwise making available of the said devices. Again, one discerns a judicious choice by the Council of Europe,[34] which aims at confining criminalization to the *distribution* of potentially "threatening" means, such as passwords, which can guarantee access to an information system –or parts thereof- by their very nature. None among these limitations, which serve to exclude the use of devices for legitimate purposes from the ambit of criminalization, have been adopted by the E.U. As a result, criminalization largely depends on subjective criteria, which are hard to establish.[35]

Adding to the picture, two more elements of the E.U. directive point to the broadness of its ambit: first of all, member States are required to criminalize even aiding and abetting to the offense proscribed under article 7 (article 8, par. 1). Although this requirement is also present in the Council of Europe Convention (article 11), its effect is mitigated by the discretion granted to State-parties; secondly, member States are required to criminalize attempt without exceptions (article 8, par. 2), in stark contrast to both the replaced framework decision (exempting attempted illegal access to information systems under article 5, par. 3) and the Cybercrime Convention, recognizing the right of each State-party to not apply, in whole or in part, paragraph 2 concerning attempt (article 11, par. 2 and 3). On the other hand, the exclusion of the offense of articles 6 and 7 from the ambit of attempt is a positive step (one also taken by the Council of Europe Convention).

Last but not least, it is noteworthy that every offense proscribed under the directive is only punishable when committed "without right", an element also found in the replaced framework decision and the Council of Europe Convention. Although the Council of Europe Convention leaves

---

34 *Ibid*., at 72-78.

35 Even on a European level, criminalization needs to rely on a clear-cut affirmation of a fundamental interest which incurs serious damage by the act in question: see *ECPI* (2010), at 707.

the definition of this notion –hence the decision regarding the broadness of criminalization- to State-parties, article 2(d) of the directive defines it as meaning "access […] not authorized by the owner, other right holder of the system or of part of it, or not permitted under national legislation".[36] From a purely rule-of-law standpoint, such definition appears problematic, as it effectively allows the owner –especially in the case of a contract- to even unduly restrict the free flow of information,[37] which is absolutely essential in a democratic society, thus affecting the limits of the proscribed conduct.

2.3.3. Criminal sanctions

In the exercise of the E.U.'s recognized competence to establish minimum rules concerning penalties, the directive contains specific sentences to be imposed, going further than article 13 of the Cybercrime Convention, which is confined to declaring the need for effective, proportionate and dissuasive sanctions. In addition, there are demonstrable differences even compared to the replaced framework decision, leading to an overall strengthening of criminal repression.

Under the directive, member States shall specifically ensure that every offense mentioned above (i.e. even the preparatory acts proscribed in article 7) is punishable by criminal penalties of a maximum term of imprisonment of at least two years (article 9, par. 2).[38] Aside from undermining the principle of proportionality, such provision signifies that the E.U. leans towards inflexible sentences, as it distances itself from the replaced framework decision providing maximum terms of imprisonment in a more flexible fashion (e.g. a maximum term of at least 1 to 3 years). The principle of proportionality is clearly better served by the abolished provision, in terms of both meting out penalties for each offense and delimiting each particular sentence.[39] The wider the margin of discretion, the easier it becomes for member States to align each sentence to the corresponding gravity of the offense it attaches to. Adding to the picture, the directive introduces for the first time an inflexible minimum sentence for illegal access to in-

36 See the Explanatory Report by the Council of Europe, paras. 38 and 47.
37 See *Kaiafa-Gbandi* (2007), Arm, 1084.
38 See COM (2010) 517 final, 30.9.2010, 16.
39 See pertinently *ECPI* (2009), at 709.

formation systems. Overall, it becomes evident that the trend is now to establish more stringent penalties, while reducing the margin of discretion of member States in delimiting them.

The same reasoning has been applied under article 9 paras 3 and 4 of the directive. To begin with, the said provision expands the enumeration of aggravating circumstances so as to include commission by concealing the real identity of the perpetrator and causing prejudice to the rightful identity owner (par. 5), as well as through the use of a tool designed to launch attacks affecting a significant number of information systems (para 3), or attacks causing serious damage (par. 4), or commission against a critical infrastructure information system (par. 4).

2.3.4. Assessing the E.U. policy on criminalizing attacks against information systems in a comparative context

The above analysis of the rules concerning the criminalization of attacks against information systems as adopted by the Council of Europe and the E.U., respectively, allows us to draw a conclusion relying on the following elements:

In its effort to amend its regulatory framework concerning criminal repression of attacks against information systems, the E.U. did not pay enough heed to the *ultima ratio* principle. Such principle, which directly emanates from the principle of proportionality, is well-founded in E.U. law[40] and would protect against inhibiting technological innovation or blocking the free flow of information. Taking into account the numerous possibilities for restricting criminalization as mandated under the Council of Europe Convention, one would indeed expect the E.U. to strive for more balanced solutions in repressing cybercrime, especially after the Lisbon Treaty, which enables it to bind its member States–on grounds of majority vote- to minimum rules concerning the definition of offenses and criminal sanctions,[41] i.e. impose its own choices as to the distinction between those acts that deserve punishment and those that do not.

---

40 See *Kaiafa-Gbandi* (2010), NoV, 2187, at n. 29, *Mylonopoulos* (2010), European criminal law and general principles of E.U. law, PChr, 161.

41 On this requirement as it emerges after the Lisbon Treaty see *Kaiafa-Gbandi* (2010), NoV, 2187-2190.

A close look at the preamble of the E.U. directive reveals the actual reasons behind the choices made. Prominent among the grounds for adopting the directive is the need to fight organized crime and terrorism, and sec. 3 of the preamble notes the increasing concern about the potential for terrorist or politically motivated attacks against information systems which form part of the critical infrastructure of Member States and the Union. Interestingly, however, the repression of attacks against information systems carried out in the context of organized crime or terrorism would require nothing more than *special provisions* designed to address these acts, as opposed to a blanket extension of criminal law rules.

On the other hand, the directive neither ensures respect for fundamental rights recognized under the Charter of Fundamental Rights of the European Union nor observes Union law principles, despite the preamble's reassurance to the contrary (sec. 29). Indeed, the definitions contained in the proposal do not conform to the *lex certa* requirement, which is also applicable on a European level.[42] Two pertinent examples would be the ambiguous notion of 'interception', as well as the indeterminacy surrounding 'minor cases', which are to be excluded from criminalization.[43] The principle of proportionality[44] on its part is also undermined: How is proportionality respected, when the maximum sentence is doubled on the grounds of participation in a criminal organization, despite the fact that the latter is punishable *per se*? How can proportionality possibly be served, when member States are left with virtually no margin of discretion in determining applicable sentences, thus being deprived of any competence to introduce variations based on the harm caused to different legal interests within the particular context of their own legal order?[45]

Last but not least, there is a valid concern about broadly criminalizing preparatory acts, such as the production of tools employed to commit pertinent offenses. The problem is that the directive (just like the Council of Europe Convention) also proscribes tools that are not by their very nature designed for the sole purpose of attacking information systems. Coupled with the distance between these acts (i.e. the production or possession of such tools) and the actual attack, it becomes evident that criminalization of

42 See *ECPI* (2009), 707 ff., as well as *Kaiafa-Gbandi* (2010), NoV, 2190 ff.
43 *Cf. Brodowski* (2010), ZIS, 753.
44 See *ECPI* (2009), 707, *Kaiafa-Gbandi* (2010), NoV, 2183-2184, at n. 29, *Mylonopoulos*, (2010), PChr, 161.
45 On the principle of coherence see *ECPI* (2009), at 709.

this conduct is not associated with a tangible threat to information systems, thus risking punishment over one's mere intent.[46] The fact that the E.U. (unlike the Council of Europe) does not leave room for limitations in this field makes things even worse.

Such elements cause serious concerns in view of the transposition required by member States. Let us now examine as an example, i.e. what have been the implications for the Greek legal order based on the directive described above.

3. The EU directive on attacks against information systems and the Greek legal order: points of convergence and some pertinent problems

The directive made necessary both the amendment of existing provisions[47] and the introduction of new ones into Greek law[48].

First of all the Greek legislator introduced a definition of "information systems" and "computer data" under article 13 grCC, based on the ones

---

46 *Ibid.*, at 707. On the criminalization of preparatory acts in connection with attacks against information systems see *Kaiafa-Gbandi* (2007), Arm, 1085, and, more extensively, *K. Chatziioannou*, The criminalization of hacking tools as a reasonable measure of protection regarding attacks against information systems and computer data, in M. Bottis, Eug. Alexandropoulou, I. Iglezakis (eds.) (2013), Values and Freedoms in Modern Information Law and Ethics (Proccedings of the 4th International Conference of Information Law and Ethics), 123ff. Cf. also Q.-H. *Wang, L.-T. Zhang* and *M.-K. Qiao*, Online Hacker Forum Censorship: Would Banning the Bad Guys Attract Good Guys?, http://hdl.hendle.net/10125/41840.

47 About the former legal framework see indicatively:*E. Vassilakis* (1993), Combating computer crime [in Greek], 74ff.; *Kaiafa-Gbandi* (2007), Arm., 1064ff.; *D. Kioupes* (1999), Criminal Law and Internet [in Greek],, 131ff.; *Chr. Mylonopoulos* (1991), Computers and criminal law [in Greek],, 39ff.; *Th. Krithara,* Criminal Law and Internet [in Greek],; *G. Lazou* (2001), Informatics and Crime [in Greek],; *Chr. Tsouramani* (2005), Elektronic criminality: the unsafe side of Internet [in Greek],; *Spinellis D.* (ed.) (2004), Computer Crimes, Cyber Terrorism, Child Pornography and Financial Crimes: Reports Presented to the Preparatory Colloquy for the Round Table II of the 17th International Congress of Penal Law (Beijing, 2004).

48 Introduced by Law 4416/2016. For a brief description of the new legal framework see *E. Vagena* (2017), The new legal framework for combating Cybercrime [in Greek], PoinDik, 31ff.

contained in the directive and the Council of Europe Convention.[49] However, he/she did not introduce a *distinct chapter* in the Criminal Code on attacks against information systems, which would include already existing provisions, like e.g. article like 370C on illegal access to computer data (in its amended form). This would highlight the confidentiality, integrity and availability of information systems and data as a distinct fundamental interest worthy of protection by criminal law.[50]

On the contrary, the Greek legislator made the choice to introduce new provisions referring to illegal system and data interference, to illegal interception as well as to their preparatory acts (Art. 292B, 292C, 381A, 381B, 370D and 370E grCC), spread in different chapters of the Criminal Code and reformed the existing provision on illegal access to computer data (Art. 370C grCC). In this way, having made the wrong choice by the non-introduction of a new chapter, the legislator multiplied at the same time the problematic provision on preparatory acts, which has been included as well in all the different amended chapters that became new or amended provisions related to the attacks against information systems. On the other hand, the provisions on the levels of the penalties to be applied are higher than the ones provided for by the EU directive (something that occurs ad-

49 See article 2(a) of the directive according which 'information system' is defined as "any device or group of inter-connected or related devices, one or more of which, pursuant to a program, automatically processes computer data, as well as computer data stored, processed, retrieved or transmitted by that device or group of devices for the purposes of their operation, use, protection and maintenance". On the other hand, article 2(b) of the directive defines 'computer data' as "any representation of facts, information or concepts in a form suitable for processing in an information system, including a program suitable for causing an information system to perform a function".

50 See *Kaiafa-Gbandi* (2007), Arm, 1077-1078, noting that both computer systems and data have indeed been elevated to the status of fundamental interests worthy of protection. To the extent that such data is stored, are accessible and can be the object of ownership rights, criminal law ought to protect both their confidentiality (namely the owner's right to restrict access thereto), and their integrity and availability (namely the owner's right to retain them in any desired form and be able to use them at will). See also *E. Symeonidou-Kastanidou*, Attacks against information systems: the EU provisions for their repression and the Greek legal order [in Greek], in Legal Tech and Data Protection (4th Panhellenic Congress) (2013), 59, 69. On information as a fundamental interest worthy of legal protection see *E. Vassilakis*, Combating computer crime, 62 ff.; also see *G. Nouskales* (2004), The criminal law protection of digital information [in Greek], in *ENOVE*, Digital Technology and the Law, 120 ff.

mittedly quite often in the Greek legal order) and at the same time no exclusion of minor cases from criminalization is foreseen. In many cases, of course, the crimes according to the provisions introduced in the Greek criminal code can be prosecuted only after a complaint has been filed by the victim. This scheme is not excluding with certainty minor cases from criminalization, as the victim may still wish their prosecution and file a complaint, while it can also exclude e.g. cases of normal gravity, which the Union has not allowed Member States to leave out of the scope of punishment.

However, the most important problem that the Greek legal order now causes, relates to the incorporation of article 7 of the directive, proscribing the preparatory acts of production, sale, procurement for use, import, possession, distribution or otherwise making available of devices employed to commit any of the above offenses. The two issues which raise concern are the extent of criminalization and the penalty to be applied. To the extent the directive retains a blanket provision covering computer programs designed or adapted primarily to facilitate the commission of any of the offenses proscribed in the directive, the problem of excessive criminalization indeed remains. However, domestic law could have narrowed down its scope by appropriately delineating the notion of acting "without right", which is a necessary element under the directive.

One way to achieve this would be to introduce an additional element, namely that the production, sale, etc. of computer programs primarily designed to attack information systems (as described in article 7 of the directive) only be carried out upon obtaining a formal permit. Aside from contributing in putting together a list of software applications that pose a genuine threat to information systems (which would enable the outlawing of some of them), such addition would help keep tabs on those producing or selling these applications, thus rendering the lack of a permit as a formal element of the proscribed conduct. Accordingly, any person producing or selling them with permission would not incur criminal liability, at least not until launching an attempt against an actual information system. On the other hand, lack of a permit would not necessarily connote that the person is acting without a right; indeed, such right might derive from other exceptional circumstances precluding wrongfulness, such as a state of necessity or even self-defense.

In addition, domestic law should follow the example of article 6, par. 2 of the Council of Europe Convention and explicitly state that every act proscribed in article 7 of the directive is justified (even absent a permit), if

carried out for the purpose of authorized testing or protection of a computer system. Such a clause would not contradict the directive, as the latter indeed requires a special intent to commit crimes which is all but absent in the situations described above.

In point of fact, one might consolidate the two limitations into a clause exempting the procurement and possession for personal use of the applications in question by the authority issuing permits, providing that such procurement shall take place for the purpose of authorized testing or protection of a computer system in the context of personal or professional use.

Finally, it must be said that article 187, par. 1 grCC (concerning participation in a criminal organization) would have to be updated so as to include the purpose of committing felonies consisting in system or data interference. Should that amendment take place, there would be no actual need to introduce the aggravating circumstance encompassed under article 9 of the directive (i.e. in case the above acts are committed within the framework of a criminal organization), as the cumulative charges for participation in a criminal organization and illegal system or data interference would ensure aggravation of the penalty anyway.

4. Instead of a conclusion

The above analysis makes it plain that the task of EU member States in adopting criminal law rules within an international context focused on the repression of cross-border crime is not an easy one. In the post-Lisbon era, the Union's ability to bind its member States has been extended so as to allow it to not only establish minimum rules concerning the definition of offenses, but also determine minimum sentences. It therefore becomes imperative for national delegations –as well as parliaments themselves- to actively engage in the European lawmaking process, so that fundamental principles of criminal law are better served, and the EU may achieve its declared goal, i.e. place the individual at the heart of its activities.[51] At the same time, it is imperative for national legislators to be bold enough, to correct -in the framework of the possibilities the Union law offers to them- the handicaps a Union legal instrument may bear. Copying the Union legislator and serving unilaterally criminalization may, of course, cause less

51 See the Preamble to the E.U. Charter of Fundamental Rights.

problems towards the EU, but this is not an attitude that serves the evolution of justice in two-tier models of criminal law like the one of the EU, where the Union and the Member States are cooperating in the legislative process, having a shared responsibility for the result to be achieved, which needs to be a balanced one, not only offering protection to legal interests but at the same time safeguarding the citizens' freedoms.

The U.S. Supreme Court's First Amendment refusal to protect children regarding sexually explicit speech on the Internet

Mark S. Kende[*]

1. Intoduction

21 years ago, the U.S. Supreme Court in *Reno v. American Civil Liberties Union* (ACLU)[1] ruled that the Communication Decency Act (CDA) violated the First Amendment. The law prohibited the transmission to minors over the Internet, or the display of material available to minors, that was sexually indecent. The Court used strict scrutiny, and found that the law was impermissibly content discriminatory, as well as overbroad and vague. Adults would be precluded from seeing huge amounts of protected speech. This was the Court's first Internet free speech case. What was striking about the majority opinion was the Court's admiration for this new technology. Traditionally, the Court treated new technologies skeptically in terms of First Amendment protection.

After a hiatus of cases in this area, the Court in *Packingham v. North Carolina*,[2] last term, struck down a state law that prohibited registered sex offenders from using commercial Internet services and related social media sites to interact with minors. Like the CDA, this law was poorly drafted so the First Amendment result was no surprise. But, unlike *Reno,* the majority employed intermediate scrutiny. The Court reasoned it did not want to impose a rigid standard, given the technology's evolving nature. Like *Reno*, however, this majority contained language celebrating the Internet as a new "revolutionary" public forum, which might mean that certain restrictions should receive strict scrutiny.

---

* James Madison Chair Professor of Constitutional Law, Director of the Drake Constitutional Law Center. Thank you to University of Wuerzburg Faculty of Law Professor Dr. Dr. Eric Hilgendorf for the opportunity to present on this topic at the University's May 2017 conference on "Digitization and the Law." And thanks to Jochen Feldle.

1 521 U.S. 844 (1997).

2 582 U.S. __ (2017).

This article addresses two issues. First, what level of scrutiny should the Court use when examining Internet free speech cases? Second, has the Court been correct to strike down most Internet speech restrictions, even though they are designed to protect children? To put it differently, has the Court adequately accounted for and balanced the interests of children in not being exposed to certain material as part of its First Amendment analysis.

Part 2 of the paper will demonstrate that the Court has generally questioned the First Amendment value of new technologies. It will also illustrate the Internet's special protection. Part 3 will examine the *Reno* case. Part 4 will examine why the Court incorrectly struck down a far better drafted law, the Child On-Line Protection Act (COPA), aimed at protecting children in *Ashcroft v. ACLU* II.[3] COPA was even closely modeled after the Supreme Court's accepted obscenity definition. Part 5 will show how the Court was also wrong in striking down a law that banned "virtual" indecent material from the Internet. Part 6 will then briefly discuss how the Internet has changed in the last 20 plus years, it will describe an Internet threats case, and it will analyze *Packingham*, which reached the right result, but still paid homage to the Internet. The conclusion will argue that the Internet does not deserve such status, despite its benefits. That's because it has many dangerous components that the Court has not appreciated, as shown by the concurring opinions in the North Carolina case. There is now even a "Dark Net"[4] that did not seem to exist at the time of *Reno.*

2. Background

Historically, the Supreme Court treated new technologies as not producing free speech. For example, in 1899, the Court decided *City of Richmond v. Southern Bell & Telegraph Co.*,[5] and ruled that a telephone company lacked the power to piggy back on the speech rights of telegraph operators

3 542 U.S. 656 (2004).

4 Brad Chacos, *Meet Darknet, the hidden anonymous underbelly of the searchable Web,* PC WORLD, Aug. 12, 2013, http://www.pcworld.com/article/2046227/meet-darknet-the-hidden-anonymous-underbelly-of-the-searchable-web.html As the Chacos article shows, it is sometimes called the "deep Web.".

5 174 U.S. 761 (1899).

because "[t]he science of telephony, as now understood, was little known as to practical utility in 1866…"

In *Mutual Film Corp. v. Industrial Commission of Ohio*,[6] from 1915, the Court ruled that films were not protected by the First Amendment because, "They are mere representations of events, of ideas, and sentiments published and known, vivid, useful, and entertaining, no doubt, but as we have said, capable of evil, having power for it, the greater because of their attractiveness and manner of exhibition." The Court did not officially grant First Amendment protection to films until 1952 in *Joseph Burstyn, Inc. v. Wilson*.[7] The Court's traditionalism is still evident by its refusal to televise its own proceedings live, no matter how important the case.

By contrast, the Digital Millennium Copyright Act of 1998 (DMCA) contains provisions that protect U.S. Internet servers and intermediaries from being liable for what people post in many circumstances, as does another statute.[8] Germany has also had a law providing limited Internet server immunity, but the German legal system apparently still allows greater protection of children from the Internet.[9]

3. Reno v. ACLU

The Court's reaction to the early Internet in 1997 was enthusiastic. Justice Stevens authored the majority in *Reno v. ACLU*[10] and touted how "anyone with access to the Internet may take advantage of a wide variety of communication and information methods." After discussing sexually explicit email, chat rooms, the Web, etc. he wrote that "[t]aken together, these tools constitute a unique medium – known to its users as "cyberspace" – located in no particular geographical location but available to anyone, anywhere in the world."[11] His enthusiasm for the technology was so high that

---

6 236 U.S. 230 (1915).
7 343 U.S. 495 (1952).
8 17 U.S.C. Secs. 512. There is also an immunity provision in the Communication Decency Act. 47 U.S.C. Sec. 230 (c)(1).
9 Sec. 5, par. 2, German Teleservices Act (server immunity privilege). The Basic Law's Freedom of Expression provision expressly discusses the interests of children unlike its U.S. counterpart. Basic Law Article 5 (2) (the Basic Law is known as the Grundgesetz in German).
10 521 U.S. 844 (1997).
11 521 U.S. at 851.

he did not acknowledge that he had written judicial decisions over the years deriding sexually indecent speech as low value in non-Internet cases.[12]

Reno involved the constitutionality of the Communications Decency Act (CDA)[13] which prohibited the sending or display of sexually indecent, but not obscene, material on the Internet in a manner accessible to children. Indecency was defined as, material "that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs." The CDA actually passed as a U.S. Senate floor amendment without committee hearings, after the conservative Senator Exon from Nebraska suddenly learned about the offensive material on the Internet.[14] There were some affirmative defenses, if a Web site used age or credit card verification to keep out children. And the CDA could not reach foreign-based indecent material.

U.S. constitutional law already treated obscenity as unprotected speech, along with fighting words, incitement, true threats, child pornography, and defamation. The U.S. Supreme Court has adopted tests for regulating each of these types of expression – creating the impression that the Court has a categorical approach.[15] A major issue in *Reno* was what level of scrutiny, or not of categorical approach should be applied to the Internet.

But the CDA actually created a conflict between the protection of children and the free speech rights of adults. Justice Stevens concluded that the law violated *Butler v. Michigan*,[16] a precedent which said that adults

---

12 Young v. American Mini Theatres, Inc, 427 U.S. 50, 70-71 (1976) (he writes there that few of us would send our sons and daughters off to war to defend "unspecified sexual activities").

13 47 U.S.C. Sec. 223 et. seq.

14 Robert Cannon, *The Legislative History of Senator Exon's Communication Decency Act: Regulating Barbarians on the Information Superhighway*, 49 FED. COMMUNICATIONS L.J. 51 (1996), http://www.cybertelecom.org/cda/cannon2.html.

15 ERWIN CHEMERINSKY, CONSTITUTIONAL LAW, PRINCIPLES AND POLICIES 1036-1037 (5TH Ed. 2015).

16 352 U.S. 380 (1957) (A Michigan man was unconstitutionally found guilty of violating a law which prohibited the production, possession, or distribution of any literature, image, or recording "containing obscene, immoral, lewd or lascivious language, or obscene, immoral, lewd or lascivious prints, pictures, figures or descriptions, tending to incite minors to violent or depraved or immoral acts, manifestly tending to the corruption of the morals of youth." Since some of this material was legal for adults to read, the Court wrote that upholding the law to protect children would be "to burn the house, to roast the pig.").

could not be forced to watch only material suitable for children. The plasticity of the technology made it fundamentally impossible to "zone off" parts of the Internet from children, so indecent sites would likely have to close otherwise. Adult free speech won.

Stevens also ranked technologies. The broadcast medium was the worst because it permeated everything. A child could turn on the wrong radio station in the car, and immediately hear George Carlin's famous indecent comedy monologue on the seven dirty "words you couldn't say on the public…airwaves."[17] But, Stevens said a child could not accidentally be exposed to indecent Internet sites due to the site warnings and age verification mechanisms. Stevens also criticized the CDA's severe criminal penalties, as well as its chilling effect, vagueness and overbreadth problems. Educational sites, e.g. for AIDS, could be banned.

In sum, the Court found that the CDA was content discriminatory and deserving of strict scrutiny, which it could not pass as it lacked narrow tailoring. Stevens analogized to an earlier technology case, *Sable Communications Inc. v. FCC*,[18] where the Court struck down a ban on 1-800 phone sex lines because the calls required affirmative acts by the viewer, and credit cards, meaning that children were already safe. The Court even treated the Internet with the same deference, or more, than newspapers.

Despite the right result, Stevens essentially ignored the Internet's dangers. I was one of the first scholars who discussed these dangers in a *Constitutional Commentary* article at the time.[19] Prosecutors in many countries have successfully convicted adults for using digital technology as a method of creating child pornography, as a way to meet children for illegal purposes, and sometimes for injuring or killing the children. This problem is worsened by the Internet's interactivity and anonymity. U.S. Depart-

---

17 Federal Communications Commission v. Pacifica Foundation, 438 U.S. 726 (1978) (Court upholds mild penalty against radio station and suggests that the station broadcast such material at night or when children will likely not be available).

18 492 U.S. 199 (1989).

19 Mark S. Kende, *The Supreme Court's Approach to the First Amendment in Cyberspace: Free Speech as Technology's Handmaiden*, 14 CONSTITUTIONAL COMMENTARY 465 (1997). Most commentators approved the decision for keeping the Internet relatively unrestricted, without paying much attention to the Internet's uniquely dangerous qualities. See e.g. Scott Shail, Note, *Reno v. ACLU: The First Congressional Attempt to Regulate Pornography on the Internet Fails First Amendment Scrutiny*, 28 UNIV. OF BALTIMORE L. REV. 272 (1998), http://scholarworks.law.ubalt.edu/ublr/vol28/iss1/6.

ment of Justice Statistics reveal that 13% of youth online users received unwanted sexual solicitations, sometimes with promises of money or other favors. The DOJ also reports that "of respondents to a survey of juvenile victims of Internet-initiated sex crimes, the majority met the predator willingly face-to-face and 93% of those encounters had included sexual contact."[20] Murders have even occurred that started with on-line contacts.[21] And there is an infamous German case where the Internet was used by a "middle class" cannibal to recruit a willing victim.[22]

Further the assumption that adults accessing indecent material does not impact children is wrong.[23] It "normalizes" the material for one thing. And postings can destroy people's reputations, or cause violence or bullying. Then there's the apparently growing problem of revenge porn.[24] It's true that parents could place filters on their children's computers. Yet any determined teenager would likely have friends with unfiltered computers, or smart phones. Moreover, tech savvy teenagers could probably dismantle filters, and other kids could steal their parent's credit card numbers. Also the sexually explicit material on the Internet can be more graphic than broadcast or cable television, and the teaser age warnings would probably make teenagers only more eager to enter this forbidden cyberspace.

---

20 U.S. Department of Justice, NSOPW, RAISING AWARENESS ABOUT SEXUAL ABUSE, FACTS AND STATISTICS, https://www.nsopw.gov/en-us/Education/FactsStatistics?AspxAutoDetectCookieSupport=1 See e.g. NBCNEWS.com, *Massive on-line pedophile ring busted by cops*, http://www.nbcnews.com/id/42108748/ns/us_news-crime_and_courts/t/massive-online-pedophile-ring-busted-cops/#.WZ3lgPL0fR8 (ring had up to 70,000 multi-national members and hundreds of children were saved).

21 *Internet killer admits murdering women he met in on-line chat rooms,* LONDON TELEGRAPH, Jan. 15, 2009. The killer was apparently German. For a list of this and other on-line related acts of violence, one can examine the entry "Internet Homicide" on Wikipedia.

22 Kate Connolly, *Cannibal filmed himself killing and eating his 'willing victim,'* THE TELEGRAPH, Aug. 14, 2003, http://www.telegraph.co.uk/news/worldnews/europe/germany/1448497/Cannibal-filmed-himself-killing-and-eating-his-willing-victim.html.

23 These problems still exist of course, despite efforts by groups to caution people. Sandy Cohen, *Adults' bad online behavior impacts teens and children,* DES MOINES REGISTER, E1, July 17, 2017.

24 CYBER CIVIL RIGHTS INITIATIVE, https://www.cybercivilrights.org/ (addresses revenge porn problem and shows legislation enacted). Danielle Citron and Mary Franks are two of the leaders on this issue in the U.S.

Other nations and courts have recognized the Internet's dangers. For example, in *Editorial Board of Pravoye Delo and Shtekel v. Ukraina*,[25] the European Court of Human Rights in 2011 wrote that:

> The risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is certainly higher than that posed by the press. Therefore, the policies governing reproduction of material from the printed media and the Internet may differ. The latter undeniably have to be adjusted according to technology's specific features in order to secure the protection and promotion of the rights and freedoms concerned.

According to a scholarly summary, this ECHR case decided that the Internet meant that "a new balance between freedom of expression and other human rights must be sought. In a nutshell, given that the Internet is bringing along unprecedented legal issues, restrictions to freedom of expression should be more broadly accepted."[26] This is certainly true regarding children.

4. Ashcroft v. ACLU II[27]

Congress then passed the Child On-Line Protection Act (COPA) which corrected the CDA's vague indecency criteria by adopting and modifying the Supreme Court's three part test for obscenity laws in *Miller v. California*.[28] Thus, COPA prohibited the knowing posting, for "commercial" purposes, of material harmful to minors e.g material that:

a) the average person, applying contemporary community standards, would find, taking the material as a whole and with respect to minors is designed to appeal to, or is designed to pander to, the prurient interest;
b) depicts, describes, or represents, in a manner patently offensive with respect to minors, an actual or simulated sexual act or sexual contact, an actual or simulated normal or perverted sexual act, or a lewd exhibition of the genitals or post-pubescent female breast; and

---

25 App no 33014/05 (ECHR May 5, 2011).
26 Oreste Pollicin and Marco Bassini, *Free speech, defamation, and limits to freedom of expression in the EU: a comparative analysis,* RESEARCH HANDBOOK ON EU INTERNET LAW, Ch. 21.
27 542 U.S. 656 (2004).
28 413 U.S. 15 (1973).

c) taken as a whole lacks serious literary, artistic, political or scientific value for minors.

The requirement that the material serve commercial purposes avoided closing down many educational sites.

COPA defined a minor as under 17, and retained affirmative defenses so the sites would not be put out of business given adult speech rights. What is odd is that Justice Kennedy authored the majority opinion striking down the law, and said he was using strict scrutiny, while Justice Breyer dissented and also claimed to be using strict scrutiny. This is an example of how free speech issues on the Internet have made First Amendment doctrine even more confusing. Indeed one scholar has described the Court's First Amendment jurisprudence as being outmoded like Ptolemy's astronomy.[29]

Specifically, Kennedy's opinion found COPA was not the least restrictive alternative. Parents could install filters on the computers. Children would be unable to access the prohibited material, yet adults still could. Moreover, parents could control what types of this material would be suitable for their children. Filters also blocked foreign Web sites.

Justice Breyer, the Court's self-proclaimed "pragmatist", however, countered that filters are a private family-type remedy that government could at best, incentivize. Yet the First Amendment's definition of "a less restrictive approach" meant that there had to be an alternative statute or legal restriction that could do a better job, not reliance on parents acting responsibly. Many parents don't. In addition, Breyer makes the indisputable point that a criminal law (like COPA) plus filters is going to deter this material more than filters alone. And, as Kennedy even admits, filters are both over and under-inclusive in damaging ways. Filters also may be unaffordable for some.

Moreover, as mentioned before, children will have friends whose parents don't install filters, or the kids will work around the filters. Breyer correctly elaborates that COPA is the best that Congress can do, especially given the *Miller* pedigree. Thus, he is de facto balancing the interests of

29 Eric M. Freedman, *A Lot More Comes Into Focus When You Remove the Lens Cap: Why Proliferating New Communications Technologies Make it Particularly Urgent for the Supreme Court to Abandon Its Inside-Out Approach to Freedom of Speech and Bring Obscenity, Fighting Words, and Group Libel Within the First Amendment*, 81 IOWA L. REV. 883, 885 (1996).

children and adults, and finding that a well-crafted statute can constitutionally block child access. Breyer's dissent is actually using intermediate scrutiny to uphold the law.

The result of Kennedy's majority opinion is problematic. Adults will not die or even suffer serious psychiatric injury without access to indecent material. And most educators believe classic books can elevate a student's sensitivity and wisdom. Thus, it is no leap to assert that degrading pornography can diminish a child's moral compass. Certainly, the Supreme Court took that view in 1968 when it prosecuted the sale to minors of indecent materials at a store in *Ginsberg v. New York*,[30] even though the definition of "indecent" was less precise than *Ashcroft II.*

So here's one surprising conclusion. It appears that in the United States, no law can constitutionally protect children from indecent material on the Internet. This ignores the dignity and other interests that the state has in children's development, though there is admittedly some dispute about the precise impact of this material on kids. Breyer's de facto balancing. and deference to Congress, seems more pragmatic. He is not letting the perfect be the enemy of the good.

By contrast to the First Amendment, Article 5(2) of the German Basic Law contains a freedom of expression section which specifies that, "These rights shall find their limits in the provision's general laws, *in provisions for the protection of younger persons*, and in the right of personal honor." Germany has also had a "Federal Department for Media Harmful to Young Persons." And there is a famous case involving the American company CompuServe, and its violation of these restrictions connected to Bavaria, which had important consequences for a German-based CompuServe executive, Felix Somm.[31]

5. Ashcroft v. Free Speech Coalition[32]

In 2002, the U.S. Supreme Court struck down a 1996 law aimed at "virtual child pornography" in *Ashcroft v. Free Speech Coalition*. The First

---

30 390 U.S. 629 (1968).

31 Cyber-Rights & Cyber-Liberties, (UK), *Update: CompuServe Ex-Official's Porn Case Conviction Reversed*, http://www.cyber-rights.org/isps/somm-dec.htm (1999).

32 535 U.S. 234 (2002).

Amendment protected this because no actual children were harmed in the making of virtual porn.

Yet Congress found that pedophiles use other children's explicit images to lure real children into thinking the interaction is ok, and Congress found that the images excite pedophiles.[33] Moreover, allowing such images would make the role of law enforcement harder, as police try to distinguish between the real and virtual.[34]

The Court then fell back on its rigid Internet approach by stating that, "While these categories may be prohibited without violating the First Amendment [defamation, incitement, obscenity, real child porn], none of them include the Child Pornography Protection Act of 1996."[35] In response to law enforcement concerns, the Court said "the causal link" between allowing these images and boosting pedophilia was only "contingent" and "indirect," and "depends upon some unquantified potential for subsequent criminal acts."[36] This also shows the Court's social science skepticism. The Court elaborated that, "The government may not prohibit speech because it increases the chance that an unlawful act will be committed at some indefinite future time."[37] But why not? This result undermines the protection of children and continues to protect the Internet unnecessarily.

So this decision is a mistake. Almost no social values are served by the category of virtual pornography. And the Court does not engage in real balancing, nor place this worthless virtual material in the child pornography category. The Court in zombie-like fashion simply adopts some inappropriate "marketplace of ideas" or "autonomy" based views of free speech, though children are involved.[38]

---

33 Id. at 241.

34 Id. at 254.

35 Id. at 246. The law was also found invalid because it banned adults from acting as minors in such films, but this was not the main problem.

36 Id. at 250.

37 Id. at 253.

38 But see United States v. Williams, 553 U.S. 285 (2008) (Supreme Court upheld a federal statutory provision criminalizing expression that encouraged the distribution and pandering of material as child pornography regardless of whether it actually showed children). Notice what was outlawed here was the language calling for illegal action, not the content of the material involved as in the *Free Speech Coalition* case. That's partly how the Supreme Court distinguished the cases, but

6. Recent Developments

Since these earlier Internet cases, "technological convergence" has exploded. One commentator has explained this in a very straightforward fashion:

> In general, convergence is a coming together of two or more distinct entities or phenomena. Technological convergence is increasingly prevalent in the information technology world; in this context, the term refers to the combination of two or more different technologies in a single device.Two of the most common examples of convergence are taking pictures with a cell phone -- which combines the functionality of a camera and a telephone -- and surfing the web on a television, which brings a task normally associated with a computer to a TV.[39]

Actually now it's more common to watch television shows or even movies on computers or smart phones. In the U.S., binge-watching an entire television series on a streaming broadband Internet site has become a strange rite of passage.[40] And Wi-Fi is used now rather than dial up or direct connect. This augments the mobility of these sites.

Another development is that millennials and other young people have decreasing concerns about privacy.[41] Concomitantly, social media and other vital sites have been established, such as Facebook, Google, Twitter, and YouTube that have brought many benefits, but contain shocking amounts of inappropriate porn, terrorist-type instructions or propaganda, and other sick material. Indeed, Google apps like Snapchat allow the images to disappear quickly.

Moreover, certain companies have almost monopolistic power reminiscent of the former "robber barons" such as Google, Amazon, Facebook,

---

the harms in the *Free Speech Coalition* case ought to have been recognized as serious enough to justify the prohibition as argued in the text.

39 Margaret Rouse, *technological convergence,* WHATIS.COM, Dec. 2016, http://searchconvergedinfrastructure.techtarget.com/definition/convergence.

40 Ann Brenoff, *The 8 Shows Everyone Over Age 50 Should Binge Watch*, HUFFINGTON POST, March 20, 2015, http://www.huffingtonpost.com/entry/best-shows-to-binge-watch_n_6856430.html.

41 Emily Badger, *Millenial Attitudes About Privacy May Change How They Feel About Cars*, WASHINGTON POST, Oct. 21, 2014, https://www.washingtonpost.com/news/wonk/wp/2014/10/21/millennials-attitudes-about-privacy-may-be-changing-how-they-feel-about-cars/?utm_term=.a3d03f826c2 c.

and Apple, which are collectively called "GAFA."[42] Microsoft is no slouch either. The companies are having a huge impact on U.S. democracy. So even though we access the Internet differently than in 1997, it still remains largely the Wild West. Another vital issue in the U.S. is that the DMCA generally gives service providers immunity for what others post. While this facilitates Internet freedom, it also precludes protecting children easily, though companies like Facebook and others have some censorship rules. But the rules apparently have problems.[43] And there is of course the Trump Administration's rejection of "Net Neutrality". The Trump Administration supports favoring or divaforing the content of certain companies, presumably based on financial and other considerations.[44]

Regarding recent case law, there has been an important Supreme Court threats case, and a North Carolina case that both protect the Internet.[45]

a. Elonis v. United States[46]

In 2015, the Court decided *Elonis*, which involved social media. Mr. Elonis was apparently an odd man whose wife had divorced him and who had also lost his job and friends as well.

---

42 Elizabeth Kolbert, *The Content of No Content,* THE NEW YORKER 42, Aug. 28, 2017. (reviewing two recent books highly criticial of the current media technology situation). Some have even argued that President Trump would never have been elected except for these technologies (think of the Wiki-Leaks dumping materials on the Internet related to Hillary Clinton).

43 For example, recent studies suggest that the rules are actually racially biased. Julia Angwin, Hannes Grassegger, *Facebook's Secret Censorship Rules Protect White Men from Hate Speech but not Black Children,* PRO PUBLICA, June 28, 2017, https://www.propublica.org/article/facebook-hate-speech-censorship-internal-documents-algorithms.

44 Cecelia Kang, *Trump's FCC Pick Quickly Targets Net Neutrality,* N.Y. TIMES, Feb. 5, 2017, https://www.nytimes.com/2017/02/05/technology/trumps-fcc-quickly-targets-net-neutrality-rules.html?_r=0.

45 It's worth mentioning that the Supreme Court did uphold a law that withheld federal funds from libraries that did not have "filters" on their computer with Internet access. United States v. American Library Ass'n, 539 U.S. 194 (2003). But this case had many other factors present beyond speech such as the government's taxing and spending power. And libraries were not mandated to install filters, as long as they did not mind losing federal funds.

46 575 U.S. __ (2015).

So he took to the Internet, especially Facebook, and posted voluminous threatening statements towards his ex-wife, his former friends, and others that included references to killing and dismembering them. Eventually, his ex-wife obtained a protective order, though these can be pretty useless as shown by the tragic U.S. Supreme Court case of *Town of Castle Rock v. Gonzalez*.[47] But Elonis was not stupid and he often interspersed his rants with comments about the First Amendment, his free speech rights, the fact that he would not actually do these things, and the fact that celebrities like Eminem made money off of record albums in which they threatened to injure people.

For example, Count II of the indictment quoted this posting of Elonis:

> "Hi, I'm Tone Elonis.
> Did you know that it's illegal for me to say I want to kill my wife?...
> It's one of the only sentences that I'm not allowed to say....
> Now it was okay for me to say it right then because I was just telling you that it's illegal for me to say I want to kill my wife....
> Um, but what's interesting is that it's very illegal to say I really, really think someone out there should kill my wife...[48]

And this is mild compared to other material. He walked a fine line on threats. Though this was not really a part of the Court's analysis in the case, it is hard to see any social value in his "violent abusive venting" theory of free speech.

He was indicted under a law that "made it a federal crime to transmit in interstate commerce"… "any communication containing any threat…to injure the person of another."[49] His defense was that the government never proved an actual intent to threaten e.g. deliberately communicate a true threat. The jury instructions simply relied on a "reasonable person's" assessment of the postings.

The Supreme Court erroneously ruled in his favor, and again left the Internet unregulated. The Court said that some federal threat statutes had been interpreted to contain an intentional threat requirement (mens rea). Instead, the Elonis jury instructions had resembled a negligent tort violation instruction – a reasonableness standard and knowledge of the act. Chief Justice Roberts said that is not enough. The Court left open the issue of whether recklessness would have sufficed. The Court said it should

---

47 545 U.S. 748 (2005).
48 135 S.Ct. 2005 (2017).
49 18 U.S.C. Sec. 875(c).

show "prudence" in these criminal law matters. Yet it also showed unjustified acceptance of terrifying threats on the Internet.

The case is puzzling in that it barely mentions the Internet. This might suggest the Court is treating the case no differently than others. But there was huge publicity before the case about the Court rendering its first Internet ruling on threats. It's as if Chief Justice Roberts wanted not to acknowledge what makes the Internet particularly dangerous. This is consistent with the cases already discussed.

By contrast, in dissent, Justice Thomas showed that the technological difference should not matter:

> Had Elonis mailed obscene materials to his wife and a kindergarten class, he could have been prosecuted irrespective of whether he intended to offend those recipients or recklessly disregard the possibility. Yet when he threatened [via the Internet] to kill his wife and a kindergarten class, his intent to terrify those recipients (or reckless disregard of that risk) suddenly becomes highly relevant. That need not – and should not – be the case.[50]

Also, by not clarifying the recklessness issue, the Court created confusion. As Justice Alito said concurring and dissenting, "Attorney and judges are left to guess." Alito further protested the Court's intent requirement:

> True threats inflict great harm and have little if any social value. A threat may cause serious emotional stress for the person threatened and those who care about that person, and a threat may lead to a violent confrontation. It is true that a communication containing a threat may include other statements that have value and are entitled to protection. But that does not justify constitutional protection for the threat itself.[51]

Interestingly, federal law makes threats against the President (which were one of Elonis' subjects) illegal regardless of intent.

b. Packingham v. North Carolina[52]

Last term, the U.S. Supreme Court struck down a law that prohibited registered sex offenders from accessing "a commercial social networking Web site where the sex offender knows that the site permits minor children

---

50 Id. at 2025.
51 2016.
52 582 U.S. ___ (2017).

to become members or to maintain personal Web pages."[53] The Court said that not all sex offenders remain pedophiles, that these individuals had served their time, and that these sites do not just pertain to sex. Indeed, the Court pointed out these sites allow people to learn about current events, find employment ads, voice their opinions in the 21st Century public square etc. These sites might help ex-cons reintegrate into society. Unlike twenty years earlier in *Reno* where strict scrutiny was used, however, Justice Kennedy said the law was so broad and poorly drafted that it could not pass intermediate scrutiny.

Kennedy's reasons for apparently using intermediate rather than strict scrutiny are interesting. Known for his flowery writing style, Justice Kennedy did not disappoint:

> While we now may be coming to the realization that the Cyber Age is a revolution of historic proportions, we cannot appreciate yet its full dimensions and vast potential to alter how we think, express ourselves, and define who we want to be. The forces and directions of the Internet are so new, so protean, and so far reaching that courts must be conscious what they say today may be obsolete tomorrow.
> This case is one of the first the Court has taken to address the relationship between the First Amendment and the modern Internet. As a result, the Court must exercise extreme caution before suggesting that the First Amendment provides scant protection for access to vast networks in that medium.[54]

The reference to the "modern" Internet appears to mean "Internet 2.0" with the Wi-Fi, ubiquitous social media, technological convergence and other recent developments mentioned previously. Then, Kennedy oddly wrote that the Court did not have to decide the "precise scope" of the law, though it clearly covered, for example, Amazon and the Washington Post.

Despite these statements, however, he also analogized cyberspace to public forums where speech rights are at their strongest. Thus, the concurring opinions agreed with his result, but said Kennedy's public forum language limited the ability of government to restrict speech even if the Internet evolves in dark directions. The public forum discussion hinted strict scrutiny. Justice Alito wrote:

> But if the entirety of the internet or even just social media sites are the 21st century equivalent of public streets and parks, then states may have little ability to restrict the sites that may be visited by even the most dangerous sex of-

53 N. C. Gen. Stat. Sec. 1 202.5.
54 Slip Op. at 6.

> fenders. May a state preclude an adult previously convicted of molesting children from visiting a dating site for teenagers? Or a site where minors communicate with each other about personal problems? The Court should be more attentive to the implications of its rhetoric for, contrary to the Court's suggestion, there are important differences between cyberspace and the physical world.[55]

As previously referenced, Alito points out that the Internet's anonymity, interactivity and ubiquity are problematic whereas parents can monitor children more readily in the physical world.

7. Conclusion

In conclusion, the Court's insistence on strict scrutiny in cases where it strikes down Internet laws designed to protect children is flawed. When children are involved, the Court should shift to a more intermediate type of scrutiny that will balance and treat children's interests as significant. This could resemble a European type proportionality analysis. The laws protecting minors and others in *Ashcroft II, Free Speech Coalition*, and *Elonis* for example, should have been upheld. To put it another way, Justice Breyer's pragmatic approach is best as even parts of Justice Kennedy's *Packinghham* opinion actually suggest when he used intermediate scrutiny. And the Court should stop treating the Internet as if it's harmless.

55 Slip Op. at 10. 137 S.Ct. 1730, 1743 (2017).

Trust: Privacy in the Digital Age

Ari Ezra Waldman[1]

Introduction

In May 2016, several Danish researchers released data on 70,000 users of the dating website, OKCupid. Those of us who have tried online dating know that profiles on OKCupid (or Match, JDate, or eHarmony) are rich in sensitive personal information. The researchers published much of it: usernames, age, gender, and location, as well as sexual orientation, fetishes, religious views, and more. Given the breadth of that information, it wouldn't take much to figure out the identities of those involved. And the researchers neither obtained consent nor anonymized the data.[2]

Mining personal data for scholarship is nothing new.[3] Online retailers do it all the time, as well, gathering everything from our browsing histories to Facebook "likes" to target us with advertisements they think we want to see.[4] Google tailors its search results based on what it learns from our behavior across platforms, sometimes discriminating against us in the

---

1 Associate Professor of Law and Director, Innovation Center for Law and Technology, New York Law School. Affiliate Scholar, Princeton University, Center for Information Technology Policy. Ph.D., Columbia University; J.D., Harvard Law School. Much of this essay is taken from the author's forthcoming book, *Privacy As Trust: Information Privacy in an Information Age*, scheduled to be published in 2018 by Cambridge University Press.

2 Woodrow Hartzog, *There Is No Such Thing as "Public" Data*, Slate (May 19, 2016, 9:15 AM), http://www.slate.com/articles/technology/future_tense/2016/05/okcupid_s_data_leak_shows_there_s_no_such_thing_as_public_data.html.

3 Taylor Hatmaker, *In 2006, Harvard Also Conducted a Facebook Study That Went Too Far*, The Daily Dot (July 12, 2014 6:55 AM), https://www.dailydot.com/debug/facebook-t3-study-tastes-ties-time/. *See also* Michael Zimmer, *"But the Data is Already Public": On the Ethics of Research in Facebook*, 12 Ethics Inf. Tech. 313 (2010).

4 Charles Duhigg, *How Companies Learn Your Secrets*, N.Y. Times Mag. (Feb. 16, 2012), http://www.nytimes.com/2012/02/19/magazine/shopping-habits.html.

process.[5] Data brokers amass vast collections of information about us gleaned from across the Web and sell it to the highest bidder. Facebook is steaming ahead with frighteningly accurate facial recognition technology based on the millions of photos we upload for our friends.[6] And marketers are using our buying patterns and GPS technology to send sale notifications directly to our phones when we pass a brick-and-mortar store.[7]

Under current law in the United States, almost anyone, whether they are over eager researchers or online advertisers, can use this data because, as a matter of law and social practice, the information is considered already public. We shared our data the moment we signed up for an account, browsed the Internet, or bought a book online.[8] We cannot put that genie back in the bottle, the argument goes, because we let it out a long time ago. Animating this approach is an outdated conception of privacy that is ill equipped to handle the disclosure demands of the digital age. We need

---

5 *See, e.g.*, Latanya Sweeney, *Discrimination in Online Ad Delivery*, Comm. ACM, May 2013, at 44.

6 Naomi Lachance, *Facebook's Facial Recognition Software Is Different from the FBI's. Here's Why*, NPR: All Tech Considered (May 18, 2016, 9:30 AM), http://www.npr.org/sections/alltechconsidered/2016/05/18/477819617/facebooks-facial-recognition-software-is-different-from-the-fbis-heres-why.

7 Chris Frey, *Revealed: How Facial Recognition Has Invaded Shops—and Your Privacy*, Guardian (Mar. 3, 2016, 07.01 EST), https://www.theguardian.com/cities/2016/mar/03/revealed-facial-recognition-software-infiltrating-cities-saks-toronto.

8 The "it's already public" defense is remarkably common. For example, the FBI has argued that its agents do not need warrants to set up stingrays, or decoy cell towers, to capture our cellphone location because they are only collecting public information in public places. *See* David Kravets, *FBI Says Warrants Not Needed to Use "Stingrays" in Public Places*, Ars Technica (Jan. 5, 2015, 2:25 PM), http://arstechnica.com/tech-policy/2015/01/fbi-says-search-warrants-not-needed-to-use-stringrays-in-public-places; *see also* Smith v. Maryland, 442 U.S. 735 (1979). Perpetrators of so-called "revenge porn," or the publication of intimate or graphic photos of others without their consent, often justify their behavior by stating that the victim sent them the photos in the first place. *See* Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 Wake Forest L. Rev. 345, 346 (2014). Similar arguments are deployed in "up skirt" photo cases, too: snapping pictures of a woman's body underneath her skirt cannot be an invasion of privacy, the theory goes, because the pictures were taken in public places. *See* Justin Jouvenal & Miles Parks, *Voyeur Charges Dropped Against Photographer at Lincoln Memorial*, Wash. Post (Oct. 9, 2014), https://www.washingtonpost.com/local/crime/voyeur-charges-dropped-against-upskirt-photographer-at-lincoln-memorial/2014/10/09/7dc90eac-4ff5-11e4-aa5e-7153e466a02d_story.html.

to change the way we think about privacy so we can better leverage law to protect it in a modern world.

As I have argued elsewhere, trust between social actors is a primary factor in our decision to share personal information with others.[9] Because we share when we trust, I argue that we should start talking about, thinking through, and operationalizing information privacy as a social norm based on trust. In the context of information sharing, trust gives us the ability to live with, yet minimize vulnerability by relying on expectations of confidentiality and discretion. So, when we share information with others in contexts of trust, that information should be protected as private. I call this argument privacy-as-trust, and it helps to adapt privacy to the digital age.

I. A New Way of Looking at Privacy

Privacy is an inherently social concept. The very idea of privacy presumes that we exist in both formal and informal relationships with others: privacy only matters after we share within those relationships. When making sharing decisions, we rely on and develop expectations about what should happen to our information, thus integrating privacy into our lives relative to other people.[10] As the law professor Robert Post described, privacy norms "rest[] not upon a perceived opposition between persons and social life, but rather upon their interdependence."[11] Privacy, then, is socially situated. It is not a way to withdraw or to limit our connection to others. It is, at its core, about the social relationships governing disclosure between and among individuals and between users and the platforms that collect, analyze, and manipulate their information for some purpose.[12]

For example, when we share the fact that we are HIV-positive with the 100 members of an HIV support community, we may expect a far greater degree of confidentiality and discretion from them than from just two ac-

---

9 Ari Ezra Waldman, *Privacy, Sharing, and Trust: The Facebook Study*, 67 Case W. Res. L. Rev. 193 (2016).

10 Sandra Petronio, Boundaries of Privacy 3 (2002).

11 Robert C. Post, *The Social Foundations of Privacy: Community and Self in the Common Law Tort*, 77 Cal. L. Rev. 957, 959 (1989).

12 Ferdinand David Schoeman, Privacy and Social Freedom 8 (1992) (Privacy is a social norm that gives people the confidence to share and the ability to develop relationships in the process.).

quaintances at work. When we whisper secrets to a good friend, we expect confidentiality even without a written agreement. We share our bank account numbers with Bank of America's website and expect that it won't be shared with online marketers. And although we may recognize that using the Internet or joining a discount loyalty program requires some disclosure, we share our information with the expectation that it will be used for the specific purpose for which we shared it. What we share, with whom we share it, and how we share it matter. In other words, something about the social context of disclosure is the key to determining what is private and what is not.[13]

That key is trust. Trust is a resource of social capital between or among two or more persons concerning the expectations that others will behave according to accepted norms.[14] Trust is the "favourable expectation regarding other people's actions and intentions,"[15] or the belief that others will behave in a predictable manner according to accepted contextual norms. For example, if Alice asks her friend Brady to hold her spare set of keys, she trusts Brady will not break in and steal from her; friends do not break in to friends' homes. When an individual speaks with relative strangers in a support group like Alcoholics Anonymous (AA), she trusts that they will not divulge her secrets; AA members are bound to keep confidences. Trust, therefore, includes a willingness to accept some risk and vulnerability toward others to grease the wheels of social activity.[16] And if I never trusted, my social life would be paralyzed. As Niklas Luhmann stated, trust begins where knowledge ends.[17] I cannot know for certain that my neighbor will not abuse her key privileges or that my fellow support

13 Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 Wash. L. Rev. 119 (2004). *See also* Helen Nissenbaum, Privacy in Context: Technology, Privacy, and the Integrity of Social Life (2010).

14 Alejandro Portes & Julia Sensenbrenner, *Embeddedness and Immigration: Notes on the Social Determinants of Economic Action*, 98 Am. J. Soc. 1320, 1332 (1993).

15 Guido Möllering, *The Nature of Trust: From Georg Simmel to a Theory of Expectation, Interpretation and Suspension*, 35 Sociology 403, 404 (2001); *see also* J. David Lewis & Andrew Weigert, *Trust as a Social Reality*, 63 Soc. Forces 967, 968 (1985).

16 Niklas Luhmann, Trust and Power 4 (1979).

17 *Id*. at 33–34; *see also* Patricia M. Doney et al., *Understanding the Influence of National Culture on the Development of Trust*, 23 Acad. Mgmt. Rev. 601, 603 (1998).

group members will keep my confidences, but the norms of those contexts tell me that they will.

Trust is the expectation that people will continue to behave according to those norms. Therefore, trust allows us to interact with and rely on others. It mitigates the vulnerability and power imbalance inherent in disclosure, allowing sharing to occur in the first place. Put another way, disclosures happen in contexts of trust, and trust is what's broken when data collection and use go too far.

Trust is what defines private contexts. Trust also mitigates the vulnerabilities inherent in disclosure. We are vulnerable to data collectors because we share a lot with all of them. They know a lot about us, down to the number of seconds our cursor hovers over a button, and releasing what they know could harm us. Furthermore, they have the money and manpower to aggregate information about our wants and needs, but we know nothing about the algorithms they use to analyze that data and predict our behavior. Data sharing, therefore, creates vulnerability and an imbalance of power. Elsewhere, as in doctor-patient or attorney-client relationships, where significant disclosures create similar power imbalances, we manage those risks with strong trust norms and powerful legal tools that protect and repair disclosure relationships. Reinvigorating information privacy in the digital age requires similar norms and legal weapons, as well. Privacy-as-trust matches the way we think about privacy with the power relationships that data sharing create.

Information privacy, I argue, is really a social construct based on trust between social sharers, between individuals and Internet intermediaries, between groups of people interacting online and offline, broadly understood. And because trust both encourages the sharing and openness we need in society and because breaches of privacy are experienced as breaches of trust, privacy law—the collective judicial decisions, legislative enactments, and supporting policy arguments regulating disclosures, searches and seizures, data aggregation, and other aspects of informational knowledge about us—should be focused on protecting and repairing relationships of trust. In short, the only way to reestablish the balance of power between sharers and data collectors is to leverage law to enforce disclosure's trust norms: one can be held liable for invasion of privacy if he further disseminates information that was originally shared in a context that manifests trust.

II. Applying Privacy-As-Trust: A Case Study

United States privacy law today is, for the most part, structured around concepts of autonomy, choice, and individual rights.[18] Judges deny recovery even when data collectors misuse our information because we supposedly made the free and voluntary choice to share our data in the first place.[19] Therefore, we assumed the risk that our information could be further disseminated and shared.[20] Previously disclosed information is, in this view, no longer private. And on the assumption that we make rational privacy and disclosure decisions, federal and state privacy laws focus much of their energy on requiring data collectors to draft and publish privacy policies that list, in tortuous detail, the companies' data use practices.[21] Were it not for the Federal Trade Commission's robust privacy enforcement, data collectors would have few, if any other responsibilities with respect to our data after disclosure.

Privacy-as-trust would reorient privacy law away from a narrow focus on individual choice to disclosure relationships. In this section, I briefly discuss one example of what that means. Privacy law is a multifaceted animal; it is, among others things, a collection of common law responsibilities, court decisions, federal and states statutes, and regulatory enforcement actions that manages the rights and responsibilities of citizens and data collectors alike. This section uses one case study—the legal obligations data collectors have to consumers—to tease out some of the effects of privacy-as-trust on one facet of privacy and information law. Overall, the result of approaching privacy law as a protector of trusted relationships is to more effectively protect privacy in an information age where data sharing is inevitable, ongoing, and extensive.

---

18 Ari Ezra Waldman, *Privacy As Trust: Sharing Personal Information in a Networked World*, 69 U. Miami. L. Rev. 559, 565-85 (2015).

19 There are too many examples of this to list here. *See, e.g*., Dwyer v. American Express Co., 652 NE.2 d 1351 (Ill. App. Ct. 1995); Gill v. Hearst Pub., Co., 253 P. 2 d 441 (Cal. 1953); *In re* Nw. Airlines Privacy Litig., No. Civ. 04-126, 2004 WL 1278459 (D. Minn. June 6, 2004).

20 Smith v. Maryland, 442 U.S. 735, 744 (1979).

21 *See* Ari Ezra Waldman, *Privacy, Notice, and Design*, 20 Stanford Tech. L. Rev. 129 (2018).

A. The Current Approach: Notice and Choice

Companies that collect, aggregate, analyze, and share our information have considerable power over us. But under current United States law, their responsibilities are minimal, their power essentially unlimited. That is because our relationship to data collectors is based on principles of privacy-as-autonomy. Although the rules vary to some extent by industry,[22] the general approach is the same: on the theory that we have the right to decide for ourselves how and when to disclose our information, data collectors are required to provide us with both a comprehensive list of their data use practices and the opportunity to opt out and use another platform. This regime is called "notice and choice," and it is woefully inadequate.

As a governing legal regime, notice-and-choice is self-explanatory. Companies that collect our data are supposed to tell us what information they collect, how and for what purpose they collect it, and with whom they share it. That's the notice part. We then have the opportunity to opt out.[23] That, or the option to use another platform, is the choice.

Notice-and-choice makes sense as the limits of platform responsibility if we understand privacy through a lens of autonomy and choice. At its core, notice-and-choice is a doctrine of informed consent premised on autonomous decision-making: provide us with all the information we need in a privacy policy and allow us the freedom to make our own informed decisions. If companies disclose the details of their data use practices, the argument goes, disclosure decisions will be rational exercises of our power to exercise control over our information.[24]

---

22 The Health Insurance Portability and Accountability Act (HIPAA), for example, governs the collection, storage, and sharing of certain types of health and medical information. The Children's Online Privacy Protection Act (COPPA) applies to platforms that collect information about children 13-years-old or younger. And the Gramm-Leach-Bliley Act sets out rules for information management for some financial institutions. These statutes have somewhat different rules, with each imposing additional restrictions on data sharing in certain contexts.

23 Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 Colum. L. Rev. 583, 592 (2014).

24 *See* Ryan Calo, *Against Notice Skepticism in Privacy (and Elsewhere)*, 87 Notre Dame L. Rev. 1027, 1049 (2012).

But notice-and-choice doesn't work. We do not make perfectly rational disclosure decisions regardless of what notice-and-choice may presume.[25] The law ignores our embodied experience and the contextual nature of privacy expectations.[26] What's more, notice-and-choice is meaningless in a world on ongoing data collection. As several chief privacy officers have said, concepts like "notice" and "consent" play "limited role[s]" in the ways their companies approach privacy questions because users cannot be expected to continuously evaluate their disclosure preferences over time.[27]

Notice-and-choice is also hopelessly underinclusive. It reflects an arbitrary and selective approach to the Fair Information Privacy Principles, which also included limitations on data collection, security requirements, a rejection of black boxes, user rights to data, and robust accountability policies.[28] There are administrative critiques, as well: it is difficult for companies to comply with a patchwork of laws, including the innumerable state laws governing data privacy, that apply to some information in the hands of some entities some of the time.

B. A New Approach: Trust

If we understood privacy as protecting relationships of trust, the obligations of data collectors would be different. Rather than limiting corporate responsibility to giving us a list of data use practices for rational privacy decision-making, privacy-as-trust recognizes that data collectors are being

---

25 *See* Alessandro Acquisti & Jens Grossklags, *What Can Behavioral Economics Teach Us About Privacy?*, *in* Digital Privacy 363, 363–64 (Alessandro Acquisti et al. eds., 2008); Alessandro Acquisti & Jens Grossklags, *Privacy and Rationality in Individual Decision Making*, 3 IEEE Security & Privacy 26 (2005).

26 "Embodied" experience refers to the phenomenological and pragmatic idea that things like comprehension, understanding, and truth are only possible through lived experience as mediated by the social structures around us. *See, e.g.*, Maurice Merleau-Ponty, Phenomenology of Perception xi (Ted Honderich ed., Colin Smith trans. 1962). It was applied to the context of cyberspace by Julie Cohen. *See, e.g.*, Julie E. Cohen, Configuring the Networked Self: Law, Code, and the Play of Everyday Practice 34-31 (2012); Julie E. Cohen, *Cyberspace As/And Space*, 107 Columb. L. Rev. 210, 226-35 (2007).

27 Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 Stan. L. Rev. 247, 266–267 (2011).

28 Org. for Econ. Co-operation & Dev., OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data 14–16 (2001).

entrusted with our information. Therefore, they should be held to a higher standard than mere notice. They are, in fact, fiduciaries with respect to our data, and should be obligated to act in a trustworthy manner. This argument, developed most recently and comprehensively by Yale Law School Professor Jack Balkin, follows directly from reorienting privacy law toward relationships of trust.

Fiduciary law is a common law construct, which means that judges developed it over time to respond to changing realities on the ground. Whereas contract law sets out the obligations of parties formally bound in voluntary agreements and tort law establishes the background rules of social interaction, fiduciary law focuses on a few special relationships that are based on trust and confidence. In short, a fiduciary has special obligations of loyalty and trustworthiness. A client puts his trust in a fiduciary, and the fiduciary has an obligation not to betray that trust. She must act in her client's interests, not in a way that harms him.[29] Estate managers, investment advisers, lawyers, and doctors are classic examples of fiduciaries: They handle their clients' money, secrets, and livelihoods under duties of loyalty and care.[30]

As Balkin explains, fiduciary duties are "duties of trust." Even the word "fiduciary" comes from the Latin word for "trust." And, as I argued in Chapter 5, "trust and confidence are centrally concerned with the collection, analysis, use, and disclosure of information."[31] Therefore, those that handle our personal information, whether doctors, lawyers, or an online social network, have "special duties with respect" to our information. These parties are "information fiduciaries."[32] Several other leading privacy law scholars agree. In *The Digital Person*, Daniel Solove argued that businesses that are collecting personal information from us should "stand in a fiduciary relationship with us."[33] And in a blog post at Concurring Opinions, the law professor Danielle Keats Citron suggested that a fidu-

---

29 Deborah A. DeMott, *Beyond Metaphor: An Analysis of Fiduciary Obligation*, 1988 Duke L.J. 879, 882.

30 Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U. C. Davis L. Rev. 1183, 1207-08 (2016).

31 *Id*.

32 *Id*. at 1208-09.

33 Daniel J. Solove, The Digital Person 102-03 (2004).

ciary relationship between data brokers and users would help fight the massive power imbalance online.[34]

All fiduciary relationships have two overarching similarities—namely, asymmetry and vulnerability. Doctors, lawyers, and investment managers have special skills that their clients do not. As much as we might fear hospitals, we can neither diagnose nor perform surgery on ourselves. Instead, we rely on physicians to perform these tasks. We also lack the ability to effectively monitor or evaluate our doctors' job performances. Because of these asymmetries, we are in a position of vulnerability vis-à-vis our fiduciaries: We put our information, our money, our health, and our fate in their hands.[35]

Companies like Facebook, Google, Uber, and Match.com should be considered information fiduciaries for the same reasons that doctors, estate managers, and investment analysts are considered fiduciaries. First, our relationship to these companies "involve[s] significant vulnerability." Traditional fiduciaries have special skills unavailable to their clients, just many Internet and technology companies. They know everything about us; trade secrecy keeps their algorithms hidden from us. They monitor every step we take online; we know little about how they process our information. Second, we are absolutely dependent on these companies. We cannot engage in modern life without the Internet, and our movements online are tracked as a matter of course.[36] Third, many Internet companies market themselves as experts in what they do: Facebook is the best and largest social connector,[37] Match.com calls itself "#1 in dates, relationships, and marriages,"[38] and Google is the dominant search engine and primary avenue to the World Wide Web for most Internet users.[39] And, fourth, these companies hold themselves out as trustworthy. As Kenneth Bamberger

---

34 Danielle Keats Citron, *Big Data Brokers as Fiduciaries*, Concurring Opinions (June 19, 2012), http://www.concurringopinions.com/archives/2012/06/big-data-brokers-as-fiduciaries.html.

35 Balkin, *supra* note 30, at 1216-17.

36 *Id*. at 1222.

37 Mark Zuckerberg, Facebook (Aug. 20, 2013), https://www.facebook.com/zuck/posts/10100933624710391.

38 Match, http://www.match.com/cpx/en-us/match/IndexPage (last visited Mar. 29, 2017).

39 Dan Frommer, *Google Has Run Away with the Web Search Market and Almost No One Is Chasing*, Quartz (July 25, 2014), http://qz.com/239332/google-has-run-away-with-the-web-search-market-and-almost-no-one-is-chasing.

and Deirdre Mulligan found during their groundbreaking research on privacy professionals, many leading chief privacy officers around the world felt that corporate privacy strategy was about maintaining user trust and being sufficiently flexible, adaptive, and forward looking to meet consumer expectations whatever they may be.[40] It was not about doing the least they could to prevent a lawsuit. Rather, they had to engage in ongoing management of risk and keep up with consumers' changing expectations.[41] Several CPOs talked about their jobs in fiduciary terms: they were "steward[s]" of data and "responsibl[e]" to consumers.[42] In short, several privacy leads saw their primary objective as creating and maintaining "the company's trusted relationship" with customers, employees, and society.[43]

Given this asymmetrical relationship, posting an obscure, inscrutable, and vague privacy policy is not enough to meet the fiduciary duties of care and loyalty. On top of the duty to inform, Balkin and the cyberlaw scholar Jonathan Zittrain propose "to adapt old legal ideas to create a new kind of law—one that clearly states the kinds of duties that online firms owe their end users and customers." The most basic of those duties is to "look out for the interests of the people whose data businesses regularly harvest and profit from." In other words, information fiduciaries should never act like "con men," inducing trust and then actively working against their users' interests. Balkin and Zittrain give the perfect example: Google Maps should not hold itself out as providing the "best" or "fastest" route from Logan International Airport to the Westin Copley and then deliver a route that drives passes an IHOP simply because IHOP paid Google $20.[44] Even if it never explicitly promised to offer users the fastest route on Google Maps, Google and other information fiduciaries should be held accountable when they induce trust in any way and then break it.

Balkin and Zittrain add several other obligations on top of not acting like con men. Companies "would agree to a set of fair information practices, including security and privacy guarantees, and disclosure of

---

40 Kenneth A. Bamberger & Deirdre K. Mulligan, Privacy on the Ground 59, 65, 67 (2015).

41 *Id*. 67, 68.

42 *Id*. at 66.

43 *Id*. at 67.

44 Jack M. Balkin & Jonathan Zittrain, *A Grand Bargain to Make Tech Companies Trustworthy*, Atlantic (Oct. 3, 2016), http://www.theatlantic.com/technology/archive/2016/10/information-fiduciary/502346.

breaches. They would promise not to leverage personal data to unfairly discriminate against or abuse the trust of end users." And here's the kicker: "And they would not sell or distribute consumer information except to those who agreed to similar rules."[45] Or, as Balkin wrote, "[w]hat information fiduciaries may not do is use the data in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm." This is the essence of privacy-as-trust. As we discussed above, trust is a resource of social capital between two or more parties concerning the expectations that others will behave according to accepted norms.[46] We share information with others, including online data collectors, with the expectation that those companies will treat our data according to prevailing norms and promises. We experience the further sale or dissemination of our data to unknown third parties as violations of our privacy precisely because such dissemination breaches the trust that allowed us to share in the first place. We know nothing about those third parties, particularly their data use practices. Under the law of information fiduciaries, online data collectors would not be allowed to share the data they collect with third parties that do not comply with the same data privacy obligations.

Conclusion

Pundits have been writing privacy's obituary for years.[47] We have been told privacy is dying for so long that the average person on the street can be excused for thinking it died years ago, alone, gasping for breath.

Privacy is only dead if we think about it narrowly. We tend to confuse privacy with secrecy, or limit the private world to the constellation of inti-

---

45 *Id*.

46 Alejandro Portes & Julia Sensenbrenner, *Embeddedness and Immigration: Notes on the Social Determinants of Economic Action*, 98 Am. J. Soc. 1320, 1332 (1993).

47 Thomas Friedman, *Four Words Going Bye-Bye*, New York Times (May 21, 2014), https://www.nytimes.com/2014/05/21/opinion/friedman-four-words-going-bye-bye.html; Marshall Kirkpatrick, *Facebook's Zuckerberg Says The Age of Privacy is Over*, Readwrite (Jan. 9, 2010), https://readwrite.com/2010/01/09/facebooks_zuckerberg_says_the_age_of_privacy_is_ov/; Polly Sprenger, *Sun on Privacy: 'Get Over It'*, Wired (Jan. 26, 1999 12:00 PM), https://www.wired.com/1999/01/sun-on-privacy-get-over-it/.

mate, sexual, or familial facets of our lives. Courts frequently (though not exclusively) do the same. We also tend to think about privacy spatially ("behind closed doors") or as the ability to exclude others from something by closing a window, locking a door, or stepping inside our homes.

In some ways, new technologies and the mandates of modern life have made this kind of privacy antiquated. It's hard to keep anything secret these days, especially since browsing the Internet is an information sharing event; our credit cards numbers, likes and dislikes, browsing histories, and purchasing patterns are collected, analyzed, and sold by websites, technology companies, and advertisers. This makes it difficult to control the flow of our information. What's more, disclosure is often a necessary prerequisite of modern social life and, for some, for access to legal rights and entitlements.

Even if we think that privacy ends at disclosure, the privacy-is-dead meme still doesn't make much sense. We still keep many things private. We wear clothes. We lock dairies. We warn others: "This stays between us." Social life functions with privacy. And yet, even these habits fail to tell the whole story. We do wear clothes, but not always in front of our romantic partners. We do write secrets down in diaries, but sometimes share them with our best friends, therapists, or relative strangers at support group meetings. We do make explicit requests for confidentiality, but often not when sharing with those with whom confidentiality is implied. In other words, we manage the flow of our information with selective disclosures based on contextual norms of trust.

So understood, privacy is very much alive. It is a fact of life so engrained in the social structure that we couldn't live without it. In my work, I try to show that privacy, at least in the information-sharing context, is not about separating from society, but rather about engaging with it on terms based on trust. We share when we trust, and we do so expecting that even though we shared information with others, it is not up for grabs for just anyone to hear, see, or use. We feel our privacy is violated when our trust is breached, like when we are induced to share or when our information is taken from one place and given to people or companies about which we know nothing. And we use trust to contextually manage our personae and the flow of our information in order to engage in social life. Information privacy, therefore, is really a trust-based social construct between social sharers, between individuals and Internet intermediaries, between groups of people interacting online and offline, broadly understood. As such, pri-

vacy law should be focused on protecting and repairing the relationships of trust that are necessary for disclosure.