Germany is NOT a democracy!

German Chancellor Angela Merkel has come under intense international scrutiny over authoritizing state attorneys to prosecute a TV comedian over a vulgar, satirical poem he performed lampooming Turkey's brutal dictator Tayyip Recep Erdogan. But the issue goes far beyond Merkel's cozying up to the tyrant in Ankara; Germany's libel and anti-insult laws have long been a weapon of choice for those seeking to suppress the marketplace of ideas. Hitler himself, prior to assuming power, was also a vicious libel plaintiff. In Germany, you can even get into free speech trouble for "libeling" the dead!

The Boehmerman case and the wrong debate about free speech law

Whenever he is not busy having Kurds killed, imprisoning journalists, or denying the Armenian Genocide, Turkish strongman Erdogan is a sensitive, fragile snowflake, easily offended by the many people who laugh at his ridiculous and scary regime. Having Turkish citizens who purportedly compare him to Gollum from Lord of the Rings prosecuted apparently doesn't satisfy his urges; Recently, Erdogan's regime has attempted to muzzle the laughter in Germany to. It started off with calling in Germany's Embassador to Turkey in late March after satire show Extra 3 on Germany's state-owned TV channel NDR had run a song mocking Erdogan's human rights record, saying "a journalist who writes anything that Erdogan doesn't like, he'll be in jail by tomorrow". They had also suggested Erdogan's vision of equal rights for women consisted of cops beating up female anti-government protesters as well as the men.

It was in the context of this row that another state TV comedian, Jan Boehmermann, dedicated his show to discussing the extent of the free speech rights guaranteed on paper by

Article 5 of the German Basic Law. He highlighted that laws draw the limit of the permissible at a legal concept known as *Smäh-Kritik,* vilifying criticism. He said he would perform a poem named after the concept to exemplify that, and introduced it saying "what comes next would be forbidden in Germany". Then he went on to read out a vulgar text hyperbolically accusing Erdogan, among many other things, of fellating with a "hundred sheep", having a small penis, smelling worse than the fart of a pig and watching child porn as well as beating women. He concluded his poem saying, "this is what you can't say in Germany".

The rest is history. Erdogan complained about the poem under two separate German anti-insult laws, firstly the arcane Article 103 of the criminal code, banning "the insulting of foreign heads or institutions of state" (which requires authorization by the government for prosecution to occur) and then secondly filed a legal request for prosecution under the regular law banning insults against persons, Article 185 of the criminal code (which any person can use, without any special authorization). Merkel's embattled government then issued the authorization for prosecution under Article 103, much to the surprise of press commentators. They had argued the second complaint was a "bridge" over politically hot waters that Erdogan had built for Merkel, allowing her to refuse to issue the controversial authorization under the arcane and unpopular Article 103, which even she herself has said she intends to repeal soon, but still ensuring criminal charges against comedian Boehmerman could proceed under a different law

The attack on Boehmerman's speech rights is not the first time Article 103 has been used to suppress democratic speech at the behest of the powerful. In
the 1960s it has used so frequently to persecute pro-democracy movement refugees from Iran that itbecame known as the "Shah-article". In the 1980s it was used tolegitimize police action

against protests who held up a banner describing Pinochet's murderous regime in Chile as a "gang of murderers", a historically accurate statement. The court's chilling justification: if police had not intervened to confiscate the banner, "the correct bilateral relations between Germany and Chile would have suffered to a not insignificant degree". In 2003, the president of police in Potsdam, a suburb of Berlin, wanted to use to law to prosecute an Iraq Waropponent who installed a "Bush Fuck You" placard at his home in an upscale neighborhood close to the German capital. Bush hadn't complained (so no prosecution went ahead), but well-to-do neighbors had not taken to the sign favorably. The threat of prosecution no doubt sent a chill down the war opponent's spine, and put a smile on their face

Despite this, Boehmerman's case also shows how Germany's conversation about free speech is broken. Much of the critical public reaction has not been to defend Boehmerman's right, per se, to engage in such satire, but rather has become an exercise in not-so productive group outrage against Article 103. Politicians have described the law as a "pre-democratic" remnant of an age where insulting kings was still seen as a major crime, highlighting that the law establishes much higher maximum penalties (5 years in jail) than the regular law against insults (one year in jail). The popular Focus Magazine prominently featured a bow-tie wearing constitutional law expert arguing that this violates the principle of equality before the law, making it incompatible with Germany's Basic Law. The problem with this line of reasoning is that every moment spent discussing this redundant law is one not spent discussing the wider host of censorious, unnecessary libel laws that stifle free thought in Germany, including the very same Article 185 that could yet be used to prosecute Boehmermann. The Boehmerman case has already had a knock on effect, with a Berlin administrative court banning the reprinting of his poem for a planned demonstrationagainst "insulting goats" that free speech activists had intended to

hold outside of the Turkish embassy, although the judges did not rule on the legality of his poem more widely.

Germany Anti-Insult and Libel Laws – Anti-Democratic and Stupid

Germany has a plethora of highly restrictive libel and anti-insult laws of the sort one would more expect to find in Hitler's Nazi-Germany than Merkel's supposedly tolerant Germany. Aside from the laws already mentioned, the rarely used Article 189 bans the "disparagement of the memory of the dead", Article 188 establishes particularly high penalties for "smearing and defaming" a "person involved in political life" if the speech in question is connected to the person's political activities and "makes their public work significantly harder". Article 192 explicitly says that the truth of a statement does not preclude it from constituting an illegal, punishable form of expression if it is insulting in the context of the way the statement was made. Underlying these laws is the idea that people have "personality rights" (Persönlichkeitsrechte) that a democratic state is obliged to protect from being compromised by demeaning speech.

Much of this can be traced down to the haste and post-war compromise with which the Basic Law, (then Western-) Germany's quasi-constitution was developed in the late 1940s after the fall of Hitler's Nazi dictatorship. Article 5, its' provision on free speech, reflects this perfectly. It states that everyone shall have a right to freedom of expression, information and art, without the existence of censorship, but then goes on to qualify this, making clear: "These rights shall find their limits in the provisions of general laws, in provisions for the protection of young persons, and in the right to personal honour". Theodor Heuss, a deputy to the 1948 parliamentary council that drafted the Basic Law, later said Article 5's limiting provisions were consciously vague and implied that the "right to personal honour" arose out of an egalitarian desire to ensure that the same protections against

smears would not just be available to officials of the state (as had de facto been the case in Nazi Germany, where the dignity of dissidents and democrats had not been respected by the state), but to all people.

This ties in with the Basic Law's wider rhetoric of the "inviolability of the dignity of man", a vague and unspecific platitude that would no doubt have been acceptable to both socialists and conservatives in post-Hitler West Germany. The Basic Law was originally, as it itself stated, intended to be only a compromise placeholder until such a time as a reunified Germany could pass a new constitution. But, given that the Basic Law gradually became a powerful emotive symbol of a new, post-totalitarian sense of Germanness, there little chance of this happening, and Germans will remain stuck with its inadequate free speech protections.

But the historical lack of emphasis on true free speech still does not explain the reluctance of Germany's current political, social and literary elites to demand a long-overdue expansion of speech rights. An understanding of this must be found elsewhere. An opinion piece penned by the editor-in-chief of Berlin's well-regarded, intellectual Berliner Zeitung exemplifies what many in Germany's cultural elites think about the Boehmerman case. Peter Huth wrote "Merkel did everything right… Even if there is a guilty verdict, Boehmermann will easily be able to live with the fine". It is unquestionably true that with a good (expensive) lawyer, waves of public support and a well-regarded professional background, no German TV presenter or big-league newspaper editor is likely to face jail or financially crippling fines for any insults he/she may throw at anyone. The almost certain knowledge that they themselves will never face such a predicament is exactly why many in Germany's powerful cultural and political elites find it so difficult grasp the chilling, censoring effect Germany's anti-insult laws can have on those less privileged financially, socially or professionally; Local bloggers, small

town newspapers, court case defendants, dissident refugees and historical researchers who already live on the economic margins of society but are the lifeblood of public debate. To many of these people, even the threat of a time-consuming police investigation or state prosecution can be the determining factor in not pursuing a news story, not expressing their opinion or even not exercising their fundamental due process rights.

Far from the egalitarian impulse that supposedly led to the constitutional "right to personal honour", in practice, Germany's anti-insult laws give immense power to officials to threaten small-time critics and trouble-makers who hold inconvenient opinions with legal repercussions. In 2014, a local court in the Rhineland region of Germany imposed a 6 month jail sentence for "insults" on an elderly man who had spent years writing letters to officials complaining, allegedly in crude and sometimes sexist terms, of inefficiency, ineptitude and of alleged corruption. Meanwhile, In the Schwarzwald region, an unemployed man who was dependent on social assistance received a 3 month jail sentence for using an insulting word in a telephone conversation with a local government official by whom he was told that more paperwork was needed before a permit he had requested could be issued. Last year, Germany's Constitutional Court overturned a guilty verdictissued by a local court under the anti-insults laws against a woman who encountered police while wearing a "fuck cps" sticker. The local court had characterized this as an expression impacting the "social worth of the affected persons in their official capacity and reducing it". In the 1990s, the Constitutional Court famously overturned a similar conviction against someone who had displayed a banner saying in (bad) English " a soldier is a murder [sic]", although the decision appears to be partially based on the reasoning that 'a soldier' did not specify troops from any specific national army or regiment in particular. Nonetheless, a regional higher court found that shouting "ACAB" while pointing at an

individual police officer is an illegal and specific insult.

In 2008, a small-time hotel operator who had been detained on charges of unlicensed commerce, was visited by a police inspector in jail who informed him that prosecutors had just obtained and fulfilled a search warrant for his private apartment. The hotel operator protested vigorously to the police inspector. He said that his lawyer should have been present during the search, and called the state prosecutor who had requested the search warrant a "breaker of the law whose days in the judicial system are counted". He was later investigated, prosecuted and convicted by a county court of "disparaging criticism" and "defamation" towards the state prosecutor for saying this, as well as of other charges unrelated to those comments, but an appeals court eventually overturned the verdict in 2011. Criminal charges of "smearing" (*Verleumdung*) were also used by the state to prosecute a victim of child sexual abuse who has forced to work in an illegal child brothel in the 1990s. Mandy K. had claimed in an interview with prosecutors investigating the case and publically, that that a senior judge had been among those visiting the brothel as a client. Her case sparked a national debate about allegations of judicial corruption as well as police attitudes to victims of sexual assault, and there is no record of her being convicted of the charges. But even being investigated by police and taken to court is a time-consuming, costly experience that discourages critical expression in the face of officialdom.

Germany's libel laws also have an unfortunate history of stifling the discussion of vital political topics. One of contemporary Germany's most prominent far-left politicians, Gregor Gysi, has, since the 1990s, faced allegations of having collaborated with communist Eastern Germany's feared Stasi 'state security' agency to inform on his clients, some of whom were dissidents, while he was a solicitor in Eastern Germany prior to re-unification. He vehemently denies the allegations,

which have never been proven, and became known as the "red law-suit monger" in 1990s over his successful efforts to sue those making such allegations for defamation. Despite the fact that a parliamentary committee of inquiry had deemed the allegations of informal collaboration with state security to be credible and had accused Gysi of being included in an effort to bring about the
"as-effective-as-possible suppression of the democratic opposition in the GDR [Eastern Germany]", Gysi was able to use to the judicial system to obtain an
injunction under libel law banning former Eastern German dissident Freya Klier from repeating comments suggesting that Gysi had 'not represented his clients but had instead spied on them and sought to control them together with his comrades'. Prestigious news-magazine Der Spiegel characterized the efforts to silence (in effect, if not necessarily intent) the debate using the judicial system as ultimately unsuccessful. But it also described the consequences of Gysi's lawsuits for free expression at the time in no uncertain terms; "regional newspapers reacted in a scared manner, in some editors offices one preferred to think twice about whether one should report about Gysi and the Stasi- and then didn't".

Even something as removed from day-to-day politics as historical research has come under attack under the absurd Article 188. In 2000, a Bavarian court issued an injunction banning a newspaper from making claims in a local history article that a deceased World-War-Two-era local figure had been "War-criminal who was sentenced to death". Reviewing the historical record, the court said that the deceased man had only been an "alleged war criminal", not a "Nazi-criminal", and that the death-sentence-carrying war crime conviction had been "only by Czech Courts in 1945", whichaccording to the court hadn't settled the matter of whether he was actually one. Penalties for contravention of the injunction were set at up to one month imprisonment or a not insubstantial 100000 German Marks fine. Other historical researchers have also

found their work scrutinized by Article 188 complaints submitted by angry relatives of the long-dead, although usually with less success. In 2013, a Northern German court ruled that a historical case study calling the notorious First World War German colonial military commander Lettow-Vorbeck a war criminal in regards to his activities in South-West Africa at the time did not constitute a crime, because the historical study was constitutionally protected pursuant to freedom of science. Similarly, in the 1960s, a German appeals court over-turned a five month prison sentence that had been imposed under Article 188 on a journalist who had written a historical piece questioning whether Nazi diplomat Ernst Von Rath, famously assassinated in 1938 in Paris, had been engaged in homosexual activities and had been killed in a sexual dispute. Such pointless legal action not only wastes court time, but is also a clear deterrent to research on important historical issues. If you are on a tight budget or timeline, and receive a legal threat from an incensed relative, wouldn't it seem much easier to avoid all the legal time-wasting by leaving out that sentence about the war-crimes committed by their deceased ancestor?

Of course, when vague laws exist, is there nothing to stop them from being used counter to the way lawmakers intended. Modern German Neo-Nazis have developed considerable expertise in attempting to use anti-insult laws and libel complaints to hassle journalists and anti-racist campaigners, href="http://www.spiegel.de/spiegel/print/d-13683058.html">a strategy they themselves called "penetrant legalism". Even Hitler, prior to taking power in 1933, himself filed a vexatious libel lawsuit in 1930 against Karl Rabe, the editor of the pro-democratic Munich Telegram newspaper. Rabe had been responsible for an article suggesting that Hitler had attempted to bully and threaten Crown-Prince Rupert of Bavaria in case he publically expressed criticism of a ballot measure Hitler has advocating for. Yes, that's correct, a soon-to-be dictator commanding an army of thuggish, Sturm-Abteilung death

squads had his thin skin offended by an editor who documented how he had acted like school-ground bully towards an ageing aristocrat. And the very democratic, judicial institutions he was trying to destroy humoured him by allowing him to bring his vexatious and censorious suit.

Meanwhile, Germany's cultural and political elites love pointing the finger at supposed violations of free speech and press freedom elsewhere in the world, particularly in neighboring Poland. There, their criticisms of the current Law & Justice Party government were perceived to be so out-of-touch that they attracted furious condemnation even from one of the country's main opposition leaders, the maverick Pawel Kukiz. He urged them to look "more closely at democracy in your own country". Perhaps they should take his wise words to heart and start by throwing out Germany's useless, repressive anti-insult laws. All of them.

Only a total idiot would have filed a defamation case over the term "total idiot"

The Nebraska Supreme Court reminds us in Steinhausen v. Homeservices of Nebraska, 289 Neb. 927 (Neb. 2015) that rhetorical hyperbole is not actionable as defamation. I can assure you that total idiots nationwide will fail to get the memo.

In this case, someone referred to a home inspector as a "total idiot."

Download (PDF, Unknown)

> *Nitz argues that in the context of the Hotsheets– which she refers to as a place for HomeServices agents to "express their opinions without pulling punches"38–the phrase "total idiot" is not "a factual statement that [Steinhausen] is mentally defective."39 Steinhausen responds that "[i]diocy is verifiable" and "can be defined and proved."40 He notes that "idiot" is defined in one dictionary as "a stupid person or a mentally handicapped person" and asserts that he "is neither stupid nor mentally handicapped."41 (Op. at 939)*

The Nebraska Supreme Court correctly analyzed its responsibilities in the case – something that I find lacking pretty often in trial courts nationwide.

> *The threshold question in a defamation suit is whether a reasonable fact finder could conclude that the pub- lished statements imply a provably false factual assertion.44 Statements of fact can be defamatory whereas statements of opinion–the publication of which is protected by the First Amendment–cannot.45 Put another way, "subjective impres- sions" cannot be defamatory, as contrasted with objective "expressions of verifiable facts."46 Distinguishing the two pre- sents a question of law for the trial judge to decide.47 In mak- ing this distinction, courts apply a totality of the circumstances test.48 Relevant factors include (1) whether the general tenor of the entire work negates the impression that the defendant asserted an objective fact, (2) whether the defendant used fig- urative or hyperbolic language, and (3) whether the statement is susceptible of being proved true or false.49 (Op. at 940)*

The court then explained Rhetorical Hyperbole.

> *As noted, whether the language is hyperbolic is relevant to distinguishing fact from opinion. Rhetorical hyperbole—"language that, in context, was obviously understood as an exaggeration, rather than a statement of literal fact"—is not actionable.54 In particular, "[t]he ad hominem nature of abu- sive epithets, vulgarities, and profanities,"55 which some writ- ers "use to enliven their prose,"56 indicates that the statement is hyperbole. (Op. at 941)*

Then the court showed what a total idiot you have to be to file under these facts.

> *Exercises in "name calling" (See Chang v. Cargill, Inc., 168 F. Supp. 2d 1003, 1011 (D. Minn. 2001)) generally fall under the category of rhetorical hyperbole. (See, e.g., Blomberg v. Cox Enterprises, Inc., 228 Ga. App. 178, 491 S.E.2d 430 (1997)). For example, courts have held that " 'idiot,' "(Robel v. Roundup Corp., 148 Wash. 2d 35, 56, 59 P.3d 611, 622 (2002). Accord Blouin v. Anton, 139 Vt. 618, 431 A.2d 489 (1981)) " 'raving idiot,' "(DeMoya v. Walsh, 441 So. 2d 1120, 1120 (Fla. App. 1983)) " '[i]diots [a]float,' " (Cowan v. Time, Inc., 41 Misc. 2d 198, 198, 245 N.Y.S.2d 723, 725 (N.Y. Sup. 1963)). and more vulgar variants (See Chang v. Cargill, Inc., 168 F. Supp. 2d 1003, 1011 (D. Minn. 2001)) were rude statements of opinion, rather than lay diagnoses of mental capacity. Similarly, courts have held that statements calling the plaintiff " 'stupid,' " (Chang v. Cargill) a " 'moron,' " (Purcell v. Ewing, 560 F. Supp. 2d 337, 343 (M.D. Pa. 2008)) and a " 'nincompoop' " (Stepien v. Franklin, 39 Ohio App. 3d 47, 49, 528 N.E.2d 1324, 1327 (1988)) were not actionable. Courts have also held that statements potentially referring to the plaintiff's mental health, such as "'raving maniac'" (DeMoya v. Walsh, 441 So. 2d 1120, 1120 (Fla. App. 1983)); "'pitiable lunatics'" (Thomas v. News World Communications, 681 F. Supp. 55, 64 (D.D.C.1988)); "wacko," "nut job," and*

"'hysterical'" (Lapine v. Seinfeld, 31 Misc. 3d 736, 752, 754, 918 N.Y.S.2d 313, 326, 327 (N.Y. Sup. 2011)); "'crazy'" (Stepien v. Franklin, supra note 65, 39 Ohio App. 3d at 49, 528 N.E.2d at 1327); and "crank," (See Dilworth v. Dudley, 75 F.3d 307 (7th Cir. 1996)) were statements of opinion. (Op. at 941-942) (citations added in from footnotes)

Cops use taser on woman while she recorded arrest of another man

"You a dumb bitch," video captures cop saying after yanking victim from car.

—

A 36-year-old Baltimore woman claims she was tased by police and arrested while filming the arrest of a man with her mobile phone, according to a lawsuit to be served on the Baltimore City Police Department as early as Thursday.

Video of the March 30 melee surfaced online this week. Police erased the 135-second recording from the woman's phone, but it was recovered from her cloud account, according to the Circuit Court for Baltimore City lawsuit (PDF), which seeks $7 million.

Download (PDF, Unknown)

Kianga Mwamba was driving home from a family gathering in March. Stopped in traffic, she began filming the nearby arrest of a man who she says was kicked by police.

“You telling me I can’t record,” the woman says on the video as police tell her to move on.

“I’ll park. I’ll park. I’ll park,” the woman is heard saying in her own recording.

All of a sudden an officer says, “Out of the car. Out of the car.”

She was yanked out. “He burning me. He burning me,” the woman is heard screaming.

The lawsuit comes as at least one state, Illinois, moves to ban the recording of the police amid calls across the nation for cops to be equipped with body cameras to help prevent future police scuffles resulting in deaths. President Barack Obama has also weighed in on the issue, announcing last week that the administration would provide $75 million in funding to police departments to purchase body cameras. Even before Obama’s announcement, local police departments were gobbling them up as fast as they could in the aftermath of the Ferguson, Missouri death of Michael Brown.

Mwamba was arrested on charges of assault for allegedly trying to run over two officers. Charges were dropped, and she suffered cuts and bruises.

At the end of the tape, an officer says, “You a dumb bitch, you know that?”

“What did I do?” she asks.

“You just tried to run over an officer,” the officer responds.

While in custody, she gave her phone to an officer to show the video that she didn’t try to run over anybody. The video was

allegedly erased from the phone in what her attorney, Joshua Insley, described in a telephone interview as a “coverup.”

The police department said in a statement that the language the officer used was “both offensive and unacceptable.”

“The video does not capture enough information to draw definitive conclusions about what transpired before, during, and after the arrest,” the department said. “What is clear is that the language used is unacceptable and will not be tolerated.”

The suit, filed last week, said the police “attacked” the woman, “dragged” her from her vehicle, and “threw her onto the street, handcuffed her, tasered her, called her a ‘dumb bitch,’ and kept her restrained.”

The suit says the officers arrested Mwamba and “threw her face-down on the street” to “prevent the disclosure of the video taken of them beating a handcuffed man.”

That handcuffed man was 27-year-old Cordell Bruce, who faces assault charges on allegations of striking an officer outside a nightclub—charges Bruce denies. The video does not capture him being beaten by police.

Supreme Court Says Law Enforcement Can’t Search Mobile Phones Without A

Warrant

The Supreme Court released its ruling in the Riley/Wurie cases that examine whether or not the police can search through your mobile phone without a warrant. Both the Riley and Wurie cases basically deal with the same issue, though one (Riley) involves a smartphone, while the other (Wurie) is about a more old-fashioned flip phone. I had significant problems with the government's arguments in defending such warrantless searches and so did the Supreme Court, which has made it clear that police **cannot** search phones without a warrant.

In short, the Supreme Court actually believes in the 4th Amendment. This ruling is likely to become a very key one in a number of other upcoming questions about where the 4th Amendment applies to new technologies. The Court recognizes that existing precedent allows for searches of *physical* containers, but thankfully declines to accept the government's argument that searching digital devices is the same thing. First, it notes that a big part of the reasoning that allowed the search of physical containers was to make sure there weren't any dangerous weapons. Here (despite the claims of some rather confused police) the Court realizes this is ridiculous.

> *Digital data stored on a cell phone cannot itself be used as a weapon to harm an arresting officer or to effectuate the arrestee's escape. Law enforcement officers remain free to examine the physical aspects of a phone to ensure that it will not be used as a weapon—say, to determine whether there is a razor blade hidden between the phone and its case. Once an officer has secured a phone and eliminated any potential physical threats, however, data on the phone can endanger no one.*

The ruling basically says that if the data on the phone is important, law enforcement can go get a warrant and then do the search later. It's not an emergency situation that needs to be viewed immediately. The court completely brushes off the argument from the government that remote wiping capability means content searches may be urgent by basically saying that it's not likely to happen very often or to be much of an issue. In short, this hypothetical situation of remotely wiping phones isn't likely to be a real problem – and notes that police have alternative ways to deal with that hypothetical "risk."

The court digs into just how different a digital device is than a physical container, and how the implications for allowing a search would be extreme.

> *Cell phones differ in both a quantitative and a qualitative sense from other objects that might be kept on an arrestee's person. The term "cell phone" is itself misleading shorthand; many of these devices are in fact minicomputers that also happen to have the capacity to be used as a telephone. They could just as easily be called cameras, video players, rolodexes, calendars, tape recorders, libraries, diaries, albums, televisions, maps, or newspapers.*
>
> *One of the most notable distinguishing features of modern cell phones is their immense storage capacity. Before cell phones, a search of a person was limited by physical realities and tended as a general matter to constitute only a narrow intrusion on privacy…. Most people cannot lug around every piece of mail they have received for the past several months, every picture they have taken, or every book or article they have read—nor would they have any reason to attempt to do so. And if they did, they would have to drag behind them a trunk of the sort held to require a search warrant in Chadwick, supra, rather than a container the size of the cigarette package in Robinson.*

More important than that is how this impacts your privacy:

> *The sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions; the same cannot be said of a photograph or two of loved ones tucked into a wallet. Third, the data on a phone can date back to the purchase of the phone, or even earlier. A person might carry in his pocket a slip of paper reminding him to call Mr. Jones; he would not carry a record of all his communications with Mr. Jones for the past several months, as would routinely be kept on a phone.*
>
> *Finally, there is an element of pervasiveness that characterizes cell phones but not physical records. Prior to the digital age, people did not typically carry a cache of sensitive personal information with them as they went about their day. Now it is the person who is not carrying a cell phone, with all that it contains, who is the exception.*

And, from that, the court notes, the world with smartphones is a very different world:

> *In 1926, Learned Hand observed … that it is "a totally different thing to search a man's pockets and use against him what they contain, from ransacking his house for everything which may incriminate him." … If his pockets contain a cell phone, however, that is no longer true. Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form— unless the phone is.*

Furthermore, the court notes that it's not just the storage on the phone that's at issue, but the fact that most phones reach out into the cloud:

> *To further complicate the scope of the privacy interests at stake, the data a user views on many modern cell phones may not in fact be stored on the device itself. Treating a cell phone as a container whose contents may be searched incident to an arrest is a bit strained as an initial matter…. But the analogy crumbles entirely when a cell phone is used to access data located elsewhere, at the tap of a screen. That is what cell phones, with increasing frequency, are designed to do by taking advantage of "cloud computing." Cloud computing is the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself. Cell phone users often may not know whether particular information is stored on the device or in the cloud, and it generally makes little difference.*

The ruling then walks through and rejects each of the attempts by the government to offer up ways in which it should be allowed to search phones. One important one involves the government's argument that the ruling in Smith v. Maryland (which we've discussed a lot – covering how there's no privacy expected in data handed to third parties) means retrieving the phone's call log is permitted. However, here the court notes this is **not** the same thing.

> *We also reject the United States' final suggestion that officers should always be able to search a phone's call log, as they did in Wurie's case. The Government relies on Smith v. Maryland,… which held that no warrant was required to use a pen register at telephone company premises to identify numbers dialed by a particular caller. The Court in that case, however, concluded that the use of a pen register was not a "search" at all under the Fourth Amendment. …. There is no dispute here that the officers engaged in a search of Wurie's cell phone. Moreover, call logs typically contain more than just phone numbers; they include any identifying information that an individual might add, such as the label "my house" in Wurie's case.*

The court also – importantly – highlights how attempts by the government to claim that looking through photographs on a phone is "analogous" to looking through photos in a wallet are not, in fact, analogous:

> *But the fact that a search in the pre-digital era could have turned up a photograph or two in a wallet does not justify a search of thousands of photos in a digital gallery. The fact that someone could have tucked a paper bank statement in a pocket does not justify a search of every bank statement from the last five years. And to make matters worse, such an analogue test would allow law enforcement to search a range of items contained on a phone, even though people would be unlikely to carry such a variety of information in physical form.*

That tidbit seems like it could be quite useful in future cases in which the government defends its collection of *bulk* data. That said, the court does note (in a footnote clearly directed at this issue) that this ruling is *not* about such bulk collections:

> *Because the United States and California agree that these cases involve searches incident to arrest, these cases do not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances.*

That said, the framework discussed in the ruling does, quite strongly, suggest that the Supreme Court will be fairly skeptical towards the government's defense of bulk collections. Now we just need to wait for a case challenging those programs to actually reach the Court.

Download (PDF, Unknown)

Why you should turn off your iPhone if the police stop you.

CAN THE POLICE COMPEL YOU TO UNLOCK YOUR PHONE? Why you should turn off your iPhone if the police stop you.

Recent advances in cryptographic technology and the widespread use of free, open-source cryptography have made encrypted information pervasive in our everyday lives. Apple and Google have both announced that their latest mobile operating systems will be encrypted and the manufacturers will be unable to decrypt the phones even if ordered to do so. Additionally, all Apple iPhones since the iPhone 3GS have used built-in encryption. This article provides a primer to encryption, and whether police officers can compel you to provide your password.

> *Officers can compel individuals to provide their fingerprint to unlock a phone.* ***The iPhone 5S, 6, 6 Plus, iPad Air 2, and iPad mini 3 are all equipped with "TouchID." Users of these devices are allowed to unlock their devices using only their fingerprints. The easiest way for users of these devices to avoid being compelled to provide their fingerprint to unlock their device is to restart the phone. Once the device is turned off, it will require a passcode on restart before TouchID will be active again.***

I. A Primer to Encryption

Encryption is the process by which information is converted from a form that can be understood by anyone (“plain text”) into a form (“ciphertext”) that only be read by someone who has the “encryption key.” In modern times, where information is commonly stored electronically, the key takes the form of a complex algorithm that converts plaintext into ciphertext. The term cryptography, which is the science of encryption and decryption, comes from the Greek words “kryptos” and “graphos,” which together mean “hidden writing.”

Encryption, in its many forms, has played an important role in keeping communications secret since humans first started sending messages to each other. Encrypted messages have been sent by means of hieroglyphics and smoke signals. Early Americans relied on encryption to keep their communications secret during the time of the American Revolution. After the Revolution, prominent figures like Benjamin Franklin and the first Chief Justice of the United States Supreme Court continued to be known for their use of encrypted documents. Benjamin Franklin invented ciphers that were used by the Continental Congress. He even went as far as printing a book on the use of ciphers. John Jay, the first Chief Justice of the Supreme Court used ciphers for all diplomatic correspondence made while he was outside of the country.

In recent years, the level of encryption available to the general public has far outpaced the government’s technological capabilities to decrypt the information. A brute force attack is an attempt to decrypt information by trying every possible key combination until the right key is found. The number of possible keys depends on the level of encryption, which is commonly measured in terms of bits. The most common level of encryption used today is 128-bit encryption. After years of studying encryption and the rate at which computers have improved, the European Network of Excellence in Technology

reported last year that it would take at least thirty years before 128-bit encryption could be defeated in a timely manner. The report was the culmination of over four years of research into encryption, brute force attacks, and increases in computational power over time. Even taking into consideration significant future projected increases in computational power, such as the advent of quantum computing, the organization expects 256-bit encryption will remain a highly recommended level of encryption for the foreseeable future.

Despite the difficulty in decrypting even 128-bit encryption, commonly available software now allows users to encrypt their data using much stronger levels of encryption. As a result of the advances in encryption technology, law enforcement agents and the intelligence community looked to the courts to compel encryption keys through court orders and grand jury subpoenas.

II. The Fifth Amendment Implications of Compelling Password Production

The Fifth Amendment protects individuals from being compelled to be witnesses against themselves. For the Fifth Amendment protection to apply, a statement must be (i) compelled, (ii) testimonial, and (iii) incriminating.

In re Boucher, the first case in federal court to deal with the compulsion of cryptographic keys, was decided in 2007. Sebastian Boucher was crossing the Canadian border into the United States when his vehicle was stopped for a routine border inspection. Officers found a laptop on the backseat of the vehicle and proceeded to access the files on the computer. The investigating officer was able to inspect the contents of the laptop without being prompted to enter a password. The officer noticed a number of files with names suggesting the

files might be child pornography. He then asked a special agent trained in recognizing child pornography to assist with the investigation. The special agent viewed the files and determined they were images and videos of child pornography.After placing Boucher under arrest, they seized his laptop computer and powered it down.

When law enforcement agents later tried to access the files on the laptop, they discovered the hard drive was encrypted and a password was required to access the hard drive when the computer was powered on. A special agent trained in computer forensics testified before a grand jury that there were no known backdoors to the encryption software Boucher had used by which law enforcement might defeat the encryption. The special agent also testified it would be virtually impossible to guess the password in any reasonable amount of time because it could take years for an automated program to try every possible encryption key combination. Based on the special agent's testimony, the grand jury subpoenaed Boucher to divulge the encryption key. Boucher refused and moved to quash the subpoena. At trial, United State Magistrate Jerome Neidermeier held that compelling Boucher to reveal his key would violate the Fifth Amendment.

On appeal, the state changed its strategy and instead of requesting production of the cryptographic key itself, the state requested that Boucher enter his cryptographic key to unlock the hard drive, thereby granting investigators access to the drive without forcing Boucher to divulge the key. The United States District Court ordered Boucher to enter his cryptographic key as requested. The court held that the Boucher had no act-of-production privilege that would protect him from providing the grand jury with an unencrypted version of the disk. The court, relying on Second Circuit precedent, ruled that although the entire contents of the hard drive was not known, it was a foregone conclusion that the disk contained evidence of child pornography since the government

could show “with reasonable particularity that it kn[ew] of the existence and location of the subpoenaed documents.”

While Boucher was required to turn over his password, the court reached its decision because the state already knew what was on the hard drive. Essentially there is a “foregone conclusion” to the Fifth Amendment privilege against self-incrimination

In 2012, the Eleventh Circuit determined that individuals cannot be compelled to decrypy hard drive contents when the defendant had not provided law enforcement information as to what is contained on the encrypted drive. *United States v. Doe (In re Grand Jury Subpoena Duces Tecum Dated March 25, 2011)*, 670 F.3d 1335 (11th Cir. 2012). The case arose after police seized computers and external hard drives they tracked using internet protocol addresses they had reason to believe contained child pornography. The defendant was held in contempt after refusing to decrypt the laptops and hard drives for law enforcement. On appeal, the Eleventh Circuit held that decryption and production of the contents of the hard drive would be testimonial and did trigger Fifth Amendment protections.

III. BIOMETRIC SECURITY: Why You Should Turn Off Your iPad/iPhone if You are Stopped

Today, phones and tablets are commonly secured using fingerprints. Computers are regularly secured with fingerprints and are sometimes encrypted with iris scans. While biometric scans offer better security to the average user, there is a distinct downside for everyday users. Unlike a password, which requires something you know to access your data, a biometric scan only requires something you have. In other words, the Fifth Amendment is not implicated in

providing a fingerprint or iris scan, where being required to provide a password would give rise to Fifth Amendment protections.

Last week in a Virginia Circuit Court judge ruled that officers can compel individuals to provide their fingerprint to unlock a phone. The defendant in that case, David Baust, was charged with an assault-strangulation case. The police had reason to believe the fight may have been recorded on Baust's phone and sought to compel him to unlock his cell phone. Judge Steven Frucci ruled that providing a fingerprint does not implicate the Fifth Amendment because fingerpritns are nontestimonial in nature. It is no different than being compelled to provide a DNA sample or a physical key: it is something you have, not something you know.

The iPhone 5S, 6, 6 Plus, iPad Air 2, and iPad mini 3 are all equipped with "TouchID." Users of these devices are allowed to unlock their devices using only their fingerprints. The easiest way for users of these devices to avoid being compelled to provide their fingerprint to unlock their device is to restart the phone. Once the device is turned off, it will require a passcode on restart before TouchID will be active again.

Comments or questions are welcome.

* indicates required field

Name:*

Email:*

Subject:*

Message:*

Submit

Virginia judge: Police can demand a suspect unlock a phone with a fingerprint

But passcodes need not be divulged as per the Fifth Amendment, court says.

A Virginia Circuit Court judge ruled on Thursday that a person does not need to provide a passcode to unlock their phone for the police. The court also ruled that demanding a suspect to provide a fingerprint to unlock a phone would be constitutional.

The ruling calls into question the privacy of some iPhone 5S, 6, and 6 Plus users who have models equipped with TouchID, the fingerprint sensor that allows the user—and ideally only the user—to unlock the phone. It is possible for users to turn TouchID unlocking off and simply use a passcode, and Apple has provided certain extra protections to prevent TouchID privacy issues—requiring the entry of a passcode if the phone hasn't been used in 48 hours, for example. But if a suspect simply uses TouchID to open their phone, police could have a window to take advantage of that when apprehending them.

The case in question this week involved a man named David Baust, who was charged in February with trying to strangle his girlfriend. The *Virginian Pilot* reports that Baust's phone might contain video of the conflict but that his phone was

locked with a passcode. Baust's attorney argued that passcodes are protected by the Fifth Amendment.

The judge agreed with Baust, though he noted in his written opinion that "giving police a fingerprint is akin to providing a DNA or handwriting sample or an actual key, which the law permits," the *Virginian Pilot* reports. "A passcode, though, requires the defendant to divulge knowledge, which the law protects against."

The ruling is interesting because it draws into relief the legal difference between a person's identity and their knowledge. The Fifth Amendment protects people from being forced to witness against themselves, and last year when Apple's TouchID fingerprint sensor was announced, the website Wired noted that fingerprints may not have the same protection as passcodes. "A communication is 'testimonial' only when it reveals the contents of your mind," Wired wrote. "We can't invoke the privilege against self-incrimination to prevent the government from collecting biometrics like fingerprints, DNA samples, or voice exemplars. Why? Because the courts have decided that this evidence doesn't reveal anything you know. It's not testimonial."

Comments or questions are welcome.

* indicates required field

Name:*

Email:*

Subject:*

Message:*

Submit

Law Enforcement Freaks Out Over Apple & Google's Decision To Encrypt Phone Info By Default

Last week, we noted that it was good news to see both Apple and Google highlight plans to encrypt certain phone information by default on new versions of their mobile operating systems, making that information no longer obtainable by those companies and, by extension, governments and law enforcement showing up with warrants and court orders. Having giant tech companies competing on how well they protect your privacy? That's new… and awesome. Except, of course, if you're law enforcement. In those cases, these announcements are apparently cause for a general freakout about how we're all going to die. From the Wall Street Journal:

> *One Justice Department official said that if the new systems work as advertised, they will make it harder, if not impossible, to solve some cases. Another said the companies have promised customers "the equivalent of a house that can't be searched, or a car trunk that could never be opened."*
>
> *Andrew Weissmann, a former Federal Bureau of Investigation general counsel, called Apple's announcement outrageous, because even a judge's decision that there is probable cause to suspect a crime has been committed won't get Apple to help retrieve potential evidence. Apple is "announcing to criminals, 'use this,' " he said. "You could have people who are defrauded, threatened, or even at the extreme, terrorists*

> *using it."*
>
> *The level of privacy described by Apple and Google is "wonderful until it's your kid who is kidnapped and being abused, and because of the technology, we can't get to them," said Ronald Hosko, who left the FBI earlier this year as the head of its criminal-investigations division. "Who's going to get lost because of this, and we're not going to crack the case?"*

That Hosko guy apparently gets around. Here he is freaking out in the Washington Post as well:

> *Ronald T. Hosko, the former head of the FBI's criminal investigative division, called the move by Apple "problematic," saying it will contribute to the steady decrease of law enforcement's ability to collect key evidence — to solve crimes and prevent them. The agency long has publicly worried about the "going dark" problem, in which the rising use of encryption across a range of services has undermined government's ability to conduct surveillance, even when it is legally authorized.*
>
> *"Our ability to act on data that does exist . . . is critical to our success," Hosko said. He suggested that it would take a major event, such as a terrorist attack, to cause the pendulum to swing back toward giving authorities access to a broad range of digital information.*

Think of the children! And the children killed by terrorists! And just be afraid! Of course, this is the usual refrain any time there's more privacy added to products, or when laws are changed to better protect privacy. And it's almost always bogus. I'm reminded of all the fretting and worries by law enforcement types about how "free WiFi" and Tor would mean that criminals could get away with all sorts of stuff. Except, as we've seen, good old fashioned police/detective work can

still let them track down criminals. The information on the phone is not the only evidence, and criminals almost always leave other trails of information.

No one has any proactive obligation to make life easier for law enforcement.

Orin Kerr, who regularly writes on privacy, technology and "cybercrime" issues, announced that he was troubled by this move, though he later downgraded his concerns to "more information needed." His initial argument was that since the *only* thing these moves appeared to do was keep out law enforcement, he couldn't see how it was helpful:

> *If I understand how it works, the only time the new design matters is when the government has a search warrant, signed by a judge, based on a finding of probable cause. Under the old operating system, Apple could execute a lawful warrant and give law enforcement the data on the phone. Under the new operating system, that warrant is a nullity. It's just a nice piece of paper with a judge's signature. Because Apple demands a warrant to decrypt a phone when it is capable of doing so, the only time Apple's inability to do that makes a difference is when the government has a valid warrant. The policy switch doesn't stop hackers, trespassers, or rogue agents. It only stops lawful investigations with lawful warrants.*
>
> *Apple's design change one it is legally authorized to make, to be clear. Apple can't intentionally obstruct justice in a specific case, but it is generally up to Apple to design its operating system as it pleases. So it's lawful on Apple's part. But here's the question to consider: How is the public interest served by a policy that only thwarts lawful search warrants?*

His "downgraded" concern comes after many people pointed out that by leaving backdoors in its technology, Apple (and

others) are also leaving open security vulnerabilities for others to exploit. He says he was under the impression that the backdoors required physical access to the phones in question, but if there were remote capabilities, perhaps Apple's move is more reasonable.

Perhaps the best response (which covers everything I was going to say before I spotted this) comes from Mark Draughn, who details "the dangerous thinking" by those like Kerr who are concerned about this. He covers the issue above about how any vulnerability left by Apple or Google is a vulnerability open to being exploited, but then makes a further (and more important) point: this isn't about them, it's about us and protecting *our* privacy:

> *You know what? I don't give a damn what Apple thinks. Or their general counsel. The data stored on my phone isn't encrypted because Apple wants it encrypted. It's encrypted because I want it encrypted. I chose this phone, and I chose to use an operating system that encrypts my data. The reason Apple can't decrypt my data is because I installed an operating system that doesn't allow them to.*
>
> *I'm writing this post on a couple of my computers that run versions of Microsoft Windows. Unsurprisingly, Apple can't decrypt the data on these computers either. That this operating system software is from Microsoft rather than Apple is beside the point. The fact is that Apple can't decrypt the data on these computers is because I've chosen to use software that doesn't allow them to. The same would be true if I was posting from my iPhone. That Apple wrote the software doesn't change my decision to encrypt.*

Furthermore, he notes that nothing Apple and Google are doing now on phones is any different than tons of software for desktop/laptop computers:

> *I've been using the encryption features in Microsoft Windows*

> *for years, and Microsoft makes it very clear that if I lose the pass code for my data, not even Microsoft can recover it. I created the encryption key, which is only stored on my computer, and I created the password that protects the key, which is only stored in my brain. Anyone that needs data on my computer has to go through me. (Actually, the practical implementation of this system has a few cracks, so it's not quite that secure, but I don't think that affects my argument. Neither does the possibility that the NSA has secretly compromised the algorithm.)*
>
> *Microsoft is not the only player in Windows encryption. Symantec offers various encryption products, and there are off-brand tools like DiskCryptor and TrueCrypt (if it ever really comes back to life). You could also switch to Linux, which has several distributions that include whole-disk encryption. You can also find software to encrypt individual documents and databases.*

In short, he points out, the choice of encrypting our data is *ours* to make. Apple or Google offering us yet another set of tools to do that sort of encryption is them offering a service that many users value. And shouldn't that be the primary reason why they're doing stuff, rather than benefiting the desires of FUD-spewing law enforcement folks?

Comments or questions are welcome.

Message:*

Submit

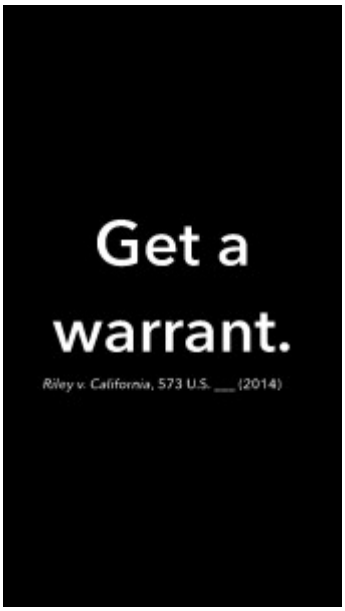
In case it’s not perfectly clear…

Get the word out there that police may not search your phone without your consent or a warrant, thanks to *Riley v. California*.

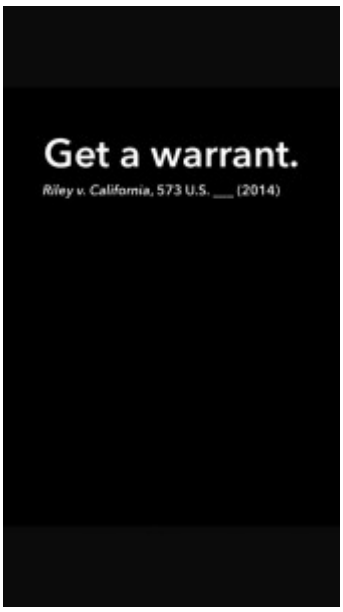
(Wikipedia here, SCOTUS opinion here, OYEZ project link here).

Download (PDF, Unknown)

Here are two lock screens for iPhone and Android. Download them and install as lock screens on your smart phones.



For the iPhone

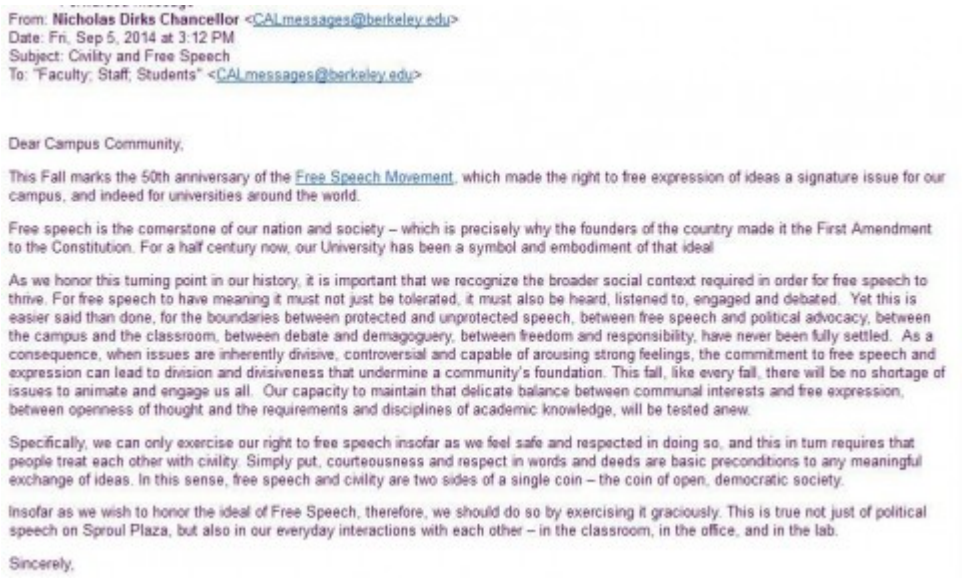


For Android

While you're at it, turn off location services.

U.C. Berkeley Chancellor Nicholas Dirks Gets Free Speech Very Wrong

Yesterday Chancellor Dirks sent an email about free speech to Berkeley students, faculty, and staff. In today's competitive publishing environment it is astonishingly difficult to distinguish yourself as an academic by being wrong about free speech, but Chancellor Dirks is equal to the challenge. His email is so very bad on every level – legally, logically, rhetorically, and philosophically – that it deserves scrutiny.



From: **Nicholas Dirks Chancellor** <CALmessages@berkeley.edu>
Date: Fri, Sep 5, 2014 at 3:12 PM
Subject: Civility and Free Speech
To: "Faculty; Staff; Students" <CALmessages@berkeley.edu>

Dear Campus Community,

This Fall marks the 50th anniversary of the Free Speech Movement, which made the right to free expression of ideas a signature issue for our campus, and indeed for universities around the world.

Free speech is the cornerstone of our nation and society – which is precisely why the founders of the country made it the First Amendment to the Constitution. For a half century now, our University has been a symbol and embodiment of that ideal.

As we honor this turning point in our history, it is important that we recognize the broader social context required in order for free speech to thrive. For free speech to have meaning it must not just be tolerated, it must also be heard, listened to, engaged and debated. Yet this is easier said than done, for the boundaries between protected and unprotected speech, between free speech and political advocacy, between the campus and the classroom, between debate and demagoguery, between freedom and responsibility, have never been fully settled. As a consequence, when issues are inherently divisive, controversial and capable of arousing strong feelings, the commitment to free speech and expression can lead to division and divisiveness that undermine a community's foundation. This fall, like every fall, there will be no shortage of issues to animate and engage us all. Our capacity to maintain that delicate balance between communal interests and free expression, between openness of thought and the requirements and disciplines of academic knowledge, will be tested anew.

Specifically, we can only exercise our right to free speech insofar as we feel safe and respected in doing so, and this in turn requires that people treat each other with civility. Simply put, courteousness and respect in words and deeds are basic preconditions to any meaningful exchange of ideas. In this sense, free speech and civility are two sides of a single coin – the coin of open, democratic society.

Insofar as we wish to honor the ideal of Free Speech, therefore, we should do so by exercising it graciously. This is true not just of political speech on Sproul Plaza, but also in our everyday interactions with each other – in the classroom, in the office, and in the lab.

Sincerely,

Let's take Chancellor Dirks' email bit by bit.

> *Dear Campus Community,*
>
> *This Fall marks the 50th anniversary of the Free Speech Movement, which made the right to free expression of ideas a signature issue for our campus, and indeed for universities around the world.*

So far, so good. Berkeley was the center of the campus free speech movement, and deserves recognition for it.

> *Free speech is the cornerstone of our nation and society – which is precisely why the founders of the country made it the First Amendment to the Constitution.*

OK. Yes, free expression is the cornerstone of American society. The "founders of the country made it the First Amendment" is awkward and imprecise writing – the founders recognized the rights to free expression and freedom of worship and protected them in what became the First Amendment. But I guess we can let that pass.

> *For a half century now, our University has been a symbol and*

> *embodiment of that ideal.*

Ehhh, sort of, partially. Berkeley's speech codes are not *unusually* bad. As you can see from the Foundation for Individual Rights in Education's page on them, Berkeley has some chillingly ambiguous speech policies, and has had its share of problematical censorship incidents. Regrettably, a mediocre free speech record does not distinguish Berkeley from the mainstream of American academia.

> *As we honor this turning point in our history,*

Wait. What turning point? Is an anniversary a turning point? We haven't established – or even stated – that Berkeley is facing a turning point. This is a null-phrase.

> *it is important that we recognize the broader social context required in order for free speech to thrive.*

Wuh-oh.

"Context" is the mother of prevarication.

The only "context required" for free speech to thrive is a society governed by the rule of law, educated about its rights and willing to enforce them.

> *For free speech to have meaning it must not just be tolerated, it must also be heard, listened to, engaged and debated.*

No.

First, observe the hidden premise Chancellor Dirks is presenting – that free speech *must* have "meaning." This implies that speech that does not have "meaning" – as defined, one presumes, by Chancellor Dirks or a committee of people

like him – then it is not "free speech," and perhaps is not entitled to protection. Dirks is smuggling a vague and easily malleable precondition to free speech.

There is no such precondition. Our rights are not limited by some free-floating test of merit or meaning. As the United States Supreme Court recently said:

> *The Government thus proposes that a claim of categorical exclusion should be considered under a simple balancing test: "Whether a given category of speech enjoys First Amendment protection depends upon a categorical balancing of the value of the speech against its societal costs." Brief for United States 8; see also id., at 12.*
>
> *As a free-floating test for First Amendment coverage, that sentence is startling and dangerous. The First Amendment's guarantee of free speech does not extend only to categories of speech that survive an ad hoc balancing of relative social costs and benefits. The First Amendment itself reflects a judgment by the American people that the benefits of its restrictions on the Government outweigh the costs. Our Constitution forecloses any attempt to revise that judgment simply on the basis that some speech is not worth it. The Constitution is not a document "prescribing limits, and declaring that those limits may be passed at pleasure." Marbury v. Madison, 1 Cranch 137, 178, 2 L.Ed. 60 (1803).*

Moreover, nobody need *listen to, engage, or debate* speech for it to be entitled to protection. If nobody wants to read, engage with, or debate the points I make in this post, I am still entitled to make them. Chancellor Dirks is implying that speech must meet an idealized model to be entitled to full protection. It doesn't. Thank goodness – because then the people who control the model control the speech.

Let's move on to his next proposition.

> *Yet this is easier said than done, for the boundaries between protected and unprotected speech, between free speech and political advocacy, between the campus and the classroom, between debate and demagoguery, between freedom and responsibility, have never been fully settled.*

No. Absolutely not.

Chancellor Dirks is using a variation on a common censor's trick – saying "well, the First Amendment doesn't protect *all* speech, and sometimes the line is blurry" to justify broad restrictions. This is akin to me walking up to you, punching you in the face without warning, and saying "well, not *all* violence is prohibited. Under some circumstances it is permissible."

Yes, the First Amendment doesn't protect everything. Yes, not every possible First Amendment question has been resolved. Yes, sometimes First Amendment analysis is complex. But most often we deal in questions that have conclusive answers. Universities would like to pretend otherwise, and strive for ambiguity where there is none, but most campus speech issues are easily resolved by anyone sincerely concerned with the rule of law. Can students hand out the United States Constitution outside of an arbitrary "free speech zone? Yes. Can public schools punish students for mere crass insults? No.

Let's turn back to some of the distinctions in that sentence from Chancellor Dirks.

> *between free speech and political advocacy*

This proposed distinction is a sign of civic illiteracy. Political advocacy is not distinct from free speech. Political advocacy is the *apotheosis* of free speech. "Speech by citizens on matters of public concern lies at the heart of the First Amendment, which 'was fashioned to assure unfettered

interchange of ideas for the bringing about of political and social changes desired by the people,'" as the Supreme Court has said. Chancellor Dirks' proposed distinction is particularly galling because the Berkeley free speech movement itself was a rejection of the argument that political advocacy was unsuited for the campus.

between debate and demagoguery

There is no "demagoguery" exception to the First Amendment. Once again, Chancellor Dirks is suggesting that expression must meet an idealized idea of speech to be protected. That's wrong. "Demagoguery" might fall outside the First Amendment, but only if it satisfies well-established exceptions – such as speech posing a clear and present danger of imminent serious lawless action.

freedom and responsibility

Advocates of "contextual" views of the First Amendment like to talk about how rights are balanced by responsibilities. But the rule of law does not support this rhetorical flourish. The Constitution imposes responsibilities on the government and rights on the people. There may be a moral responsibility to speak decently, but that responsibility is enforced by the marketplace of ideas, not by the state. Nothing about Fred Phelps' speech was morally responsible, but it was protected nonetheless.

> *As a consequence, when issues are inherently divisive, controversial and capable of arousing strong feelings, the commitment to free speech and expression can lead to division and divisiveness that undermine a community's foundation.*

This is very badly written. More importantly, it is legally incoherent and misleading. If a community is build upon the rule of law and the rights of the people, evil speech does not

threaten its foundations. If the state promotes constitutional values and citizens respect them, it is not divisive to recognize that we can condemn cruel or hurtful speech without banning it. It is only when the state arrogates to itself the right to pick and choose what speech is permitted – to "balance" the interests of the speaker and the interests of the community – that the foundations begin to crumble. That's because such a balancing is inherently inconsistent with a free and self-governing people.

> *This fall, like every fall, there will be no shortage of issues to animate and engage us all. Our capacity to maintain that delicate balance between communal interests and free expression, between openness of thought and the requirements and disciplines of academic knowledge, will be tested anew.*

The rule of law permits no "delicate" balancing between "communal interests" and free speech. As the Supreme Court noted in the quote above, the framers struck that balance in recognizing and protecting the right of free speech in the First Amendment. And though the academy may require some limits on speech to operate, no government employees enjoy such robust speech protections as university employees.

> *Specifically, we can only exercise our right to free speech insofar as we feel safe and respected in doing so,*

No. Absolutely not. Flat wrong.

Chancellor Dirks may be alluding to the statutory right to an education free of harassment. But that statutory right is narrow and yields to the strictures of the First Amendment. Students have a right to an environment free of "harassment" – but for these purposes harassment means "abuse sufficiently severe, pervasive, or persistent such that it denies or limits the student's ability to participate in or benefit from the school's program." It does not mean "words that hurt my

feelings." And a good thing, to. The University of California has demonstrated that, given the opportunity, it will silence political speech on the grounds that it makes people feel "unsafe." Nor is there any right to "feel respected." You can't confer that right on someone without depriving everyone else of their right to free expression and free association. Does a student who believes in the inherent inferiority of some races enjoy a right to "feel respected?" No. Only rights are entitled to respect, and respect is expressed not through affirming words but through the rule of law.

> *and this in turn requires that people treat each other with civility.*

No.

Civility is an admirable value. It is right and fit that we ask it of each other and impose *social* consequences upon the uncivil. But speech need not be civil to be entitled to robust protection. Berkeley's free speech movement did not seek to protect civil speech; the Vietnam war was not an occasion for civility. Paul Robert Cohen's "Fuck the Draft" jacket was uncivil, but was protected by the First Amendment nonetheless. There is nothing civil about burning the flag or picketing a funeral or being a racist, but those things are protected.

> *Simply put, courteousness and respect in words and deeds are basic preconditions to any meaningful exchange of ideas.*

Here you see Chancellor Dirks weave his tricks together. Only "meaningful" speech is worthy of protection, and only "courteous" speech is meaningful. Therefore "discourteous" and "disrespectful" speech may be punished. What speech will be deemed too discourteous or too disrespectful? That depends upon the political preferences of the people administering the rules. If those in power like your speech, it will be protected. In fact it may be protected beyond the requirements

of the First Amendment. Witness, for example, a University of California school dealing with a professor who assaulted protestors and took their sign by condemning the protestors. But if those in power don't like your speech – well. Think you have the right to burn the flag, because the United States Supreme Court says you do? That depends on the flag, friend. If your public university favors the ideas expressed in the flag you may find yourself disciplined.

> *In this sense, free speech and civility are two sides of a single coin – the coin of open, democratic society.*

This statement is arguable if "this sense" means "as an idealized vision of speech to which I'd like to encourage people to aspire." As a statement of rights, it's empty and wrong. Civility is not weighed equally with free speech. It is not a prerequisite of free speech. It is a value, an idea, to be tested in the marketplace of ideas with other vales. Free speech is often uncivil. Lenny Bruce was uncivil. "Have you no sense of decency, sir? At long last, have you left no sense of decency?" was uncivil. "I have not yet begun to fight" was uncivil. "I called you naughty darling because I do not like that other world" was uncivil. "Now, if it is deemed necessary that I should forfeit my life for the furtherance of the ends of justice, and mingle my blood further with the blood of my children and with the blood of millions in this slave country whose rights are disregarded by wicked, cruel, and unjust enactments, I submit; so let it be done!" was uncivil. The equality of all humans regardless of station has always been a deeply uncivil idea, because "civil" usually means "that which makes me comfortable." Comfortable people paint nice watercolors but otherwise don't accomplish much.

> *Insofar as we wish to honor the ideal of Free Speech, therefore, we should do so by exercising it graciously.*

Pardon my incivility, Chancellor Dirks, but I don't give a

shit whether you *wish* to honor an ideal; I care whether you will comply with the law. If you don't, you should be compelled to do so at the point of a lawsuit. You will find litigation rather uncivil.

> *This is true not just of political speech on Sproul Plaza, but also in our everyday interactions with each other – in the classroom, in the office, and in the lab.*
>
> *Sincerely,*
>
> *Nicholas Dirks*
> *Chancellor*

What should we fear more – that we might encounter rude people in the classroom, the office, and the lab, or that the state aspires to regulate our interactions in all of those places?

I don't fault Chancellor Dirks for calling for civility. It is a good thing, a decent thing, a moral thing, to treat people as we would be treated. But it is not the role of the state – or its appointee, Chancellor Dirks – to police our speech to compel it.

Perhaps you think it's frivolous to subject a casual email to such scrutiny. Perhaps you think it's like proofreading your grandchild's thank-you note. *Chancellor Dirks only meant to offer a warm and friendly aspirational statement, not a set of rules,* you might say.

But like Chancellor Dirks, I care about context. His email doesn't come in a context in which free speech is safe. Rather, it comes in the context of the modern American university, at which free speech is increasingly threatened. Those threats come not just from the censorious appetites of university officials, but from the indifference of a generation of students. Chancellor Dirks isn't just asserting limits on speech that find no support in the law. He's

encouraging the students under his tutelage to view speech as something the community should "balance." He's striking at the heart of free speech, which is how the community values it. As Learned Hand said:

> *Liberty lies in the hearts of men and women; when it dies there, no constitution, no law, no court can save it; no constitution, no law, no court can even do much to help it. While it lies there, it needs no constitution, no law, no court to save it.*

People like Chancellor Dirks don't just seek to raise a generation of civil Americans. They seek to raise a generation of Americans who look to the state to tell them what speech is acceptable. This is vile and shameful.

German Government Tries To Censor Publication Of Its List Of Censored Websites

For anybody living in the United States the story I am telling here must be strange. I am from Germany, born and grew up there. This story is not strange for me at all. I left Germany 20 years ago because of bullshit like that. Germany is not a democracy, it is an indirect democracy. This is a system where the government decides what the will of the people is. Often the Government does not ask at all the populous what they want or think.

A few weeks ago, an anonymous internet user was able to

acquire and subsequently extract a website blacklist used by Germany's Federal Department of Media Harmful to Young Children (Bundesprüfstelle für jugendgefährdende Medien [BPjM]). This un-hashed list was posted to the user's Neocities blog, along with some analysis of the blacklist's contents and a rundown on the minimal protective efforts used for the list.

The actual blacklist is much more extensive than what's published here. In fact, as is noted in the post, a majority of the list is publicly viewable.

> *The censorship list ("index") is split into various sublists:*
>
> *Sublist A: Works that are harmful to young people*
> *Sublist B: Works whose distribution is prohibited under the Strafgesetzbuch (German Criminal Code) (in the opinion of the BPjM)*
> *Sublist E: Entries prior to April 1, 2003*
> *Sublist C: All indexed virtual works harmful to young people whose distribution is prohibited under Article 4 of the Jugendmedienschutz-Staatsvertrag*
> *Sublist D: All indexed virtual works, which potentially have content whose distribution is prohibited under the Strafgesetzbuch.*
>
> *The sublists A, B and E contain about 3000 movies, 400 games, 900 printed works and 400 audio recordings. That sublists are quarterly published in the magazine "BPjM-aktuell" which can be read in any major library in Germany.*

Sublists C and D are what's been withheld from the public, even as these URLs are distributed once a month to software and hardware companies. As of the time of the posting, there were more than 3,000 URLs on the blacklist.

The leaker spotted some unusual things in the list of banned URLs. To begin with, it appears that there's very little

effort being made to keep the blacklist current.

> *On only about 50-60% of the domains on the list the questionable content is still accessible: About 10% of the domains are not registered at all, another 10% are parked domains, and about 20% don't provide any content at all (either no DNS A record, no webserver on port 80 or a redirect to another domain).*

Beyond that, the government body building the list seems to be suffering from technical ineptitude, resulting in supposedly blocked sites not being blocked at all.

> *The domain "homo.com" offers a wildcard domain which echoes anything that is entered as a subdomain on the website, eg. visiting "Fritz.homo.com" results in a webpage "Haha, Fritz is gay!". On the BPjM list there is a entryirgend.ein.name.homo.com – the German "Irgend ein Name" stands for "any name". Contrary to the belief of the BPjM public servants this doesn't work as a wildcard – just this specific domain will be blocked…*
>
> *several URLs with a wrong trailing slash:*
>
> *Death.html/*
> *welcome.htm/*
> *free/index.html/*
> *freecontent.html/*
>
> *A URL path with a trailing slash means that the part before the slash is a directory and not a file. The examples above are filenames. The entries on the list with the trailing slash are invalid and return a 404 file not found error. The correct URLs without the trailing slashes won't match the hash and are not blocked. Explanation here…*

As is inevitable when entities pursue bulk website blocking, non-offending content is part of the collateral damage.

> *[T]he complete sell list of leading online music database Discogs. Probably at one point in time there was a listing of a music album which is forbidden in Germany – this was enough to block access to the "eBay of music" for years…*

> *[A]ccording to archive.org the domain facegoo.com is since at least 3 years not an porn website anymore. Now it is the website of an iPhone App for fun picture manipulation. The startup has no chance to be listed in German search engine results at all…*

This is on top of strange and very arbitrary blockages, like a listing for the videogame Dead Island at amazon.co.uk and a few offending YouTube accounts whose account pages are blocked, but not the offending videos themselves.

Beyond that, the list covers a wide variety of offensive-to-the-German-government (and in some cases, offensive to nearly everyone) content, including "normal porn, animal porn, child/teen porn, violence, suicide, nazi or anorexia." Notably, the Wikipedia page quoted in this post points out that BPjM is an anomaly in the "free" world.

> *Germany is the only western democracy with an organization like the BPjM… **The rationales for earlier decisions to add works to the index are, in retrospect, incomprehensible reactions to moral panics**.*

With its secret list exposed, the German government has gone after Neocities in a belated attempt to keep its no-longer-secret list secret. Neocities has complied, but not without protest.

> *An anti-censorship activist, concerned citizen and security researcher has proved that the hashes are very easily reversible, and published the disclosure, including a plain-text list of the censored sites on a Neocities page. Now the*

> *German government is pressuring Neocities to take the site down, and are claiming we were breaking German (and possibly US) law by hosting a copy of the list of sites that they distribute.*

The letter from KJM (Commission for the Protection of Minors in the Media) makes some rather odd statements.

> *Two lists (containing URLs) were published on one of your blogs, namely https://bpjmleak.neocities.org/. The list of URLs contains child sexual abuse material (CSAM), animal pornography, nazi propaganda, minors in poses involving unnatural sexual emphasis and content inciting hatred, just to name a few. All of the URLs are illegal under German law. Since CSAM is also illegal under US law, we are of the opinion that this site violates the laws applying to your service and also violates your terms of conditions.*

More properly stated, the *websites* contain the offensive material, not the URLs themselves. And, as was pointed out by the person researching the list, much of what's in the list is out of date (i.e., the URL no longer contains the illegal content, domain is expired, etc.) or is ineptly targeted (typos, invalid URLs, etc.), which means the list isn't nearly as useful as the government believes.

And, if the statement about violating two countries' laws wasn't (theoretically) frightening enough, KJM goes on to claim that posting this content violates Neocities own mission statement. (No. Really.)

> *The KJM sees that neocities values anonymity and states to be uncensored. But the KJM thinks that https://bpjmleak.neocities.org/ is not what your service is intentionally for as your website states: "But our goal is clear: to enable you to harness the creativity, beauty, and power of creating your own web site. To rebuild the web we*

> *lost to monotony, and make it fun again."*

The statement is truly wondrous in its inanity, approaching the level of non sequitur. At no point does the mission statement encourage the stripping of anonymity or encourage censorship. Neocities is a platform for website construction, something KJM believes is somehow contrary to sticking up for its users and their content. Leave it to a government agency to craft one of the emptiest paragraphs to ever grace an official takedown request.

The biggest issue is the list itself, the one the government wants to keep out of the hands of the public, as Neocities points out.

> *There is apparently no legal way to challenge the list. It is decided by fiat in secret by a German government agency, and there is little or zero recourse for those falsely condemned.*

By keeping it secret – ostensibly to prevent the public from accessing illegal content – website owners are kept in the dark about the German government's censorious efforts. This sort of power is dangerous without accountability. The list is outdated and composed carelessly. Sites like Discogs are blocked off while true offenders remain uncensored because the "for the children" agency can't be bothered to ensure its slash marks are properly used or that the URL is free of typos.

Neocities has discussed this unofficially with the EFF but, as the post notes, the legal implications of this leaked list are still very murky. As a precaution the list has been removed. (It survives, for now, at the Internet Archive.) And, if given notification that the posting of the list does not violate US law, the BPjM blacklist will be reposted. Either way, Neocities states that it will not punish the end user in any way and that his/her access to the site will remain intact.

The ultimate stupidity of this debacle is the fact that the German government thinks it can undo what’s been done. By acting in this fashion, it’s only drawn more attention to the list it wants to remain a secret. Worse, it’s drawn more attention to the blog post highlighting the many failures of the list itself. It’s one thing to want to prevent access to clearly illegal material. It’s quite another to slap together a list composed of dead sites, mistyped URLs and a variety of bizarre blockings based on “incomprehensible reactions to moral panics.”