

## News and Current Events :: If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy'

**If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy' - posted by sermonindex (), on: 2013/8/15 11:52**

If you happen to send an email to one of the 400 million people who use Google's Gmail service, you shouldn't have any expectation of privacy, according to a court briefing obtained by the Consumer Watchdog website. In a motion filed last month by Google to have a class action complaint dismissed, Google's lawyers reference a 1979 ruling, holding that people who turn over information to third parties shouldn't expect that information to remain private.

From the filing (emphasis added):

Just as a sender of a letter to a business colleague cannot be surprised that the recipient's assistant opens the letter, people who use web-based email today cannot be surprised if their communications are processed by the recipient's E CS provider in the course of delivery. Indeed, "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." Smith v. Maryland, ...

read more: <http://www.sfgate.com/technology/businessinsider/article/GOOGLE-If-You-Use-Gmail-You-Have-No-Legitimate-4730587.php>

**Re: If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy' - posted by Lordoitagain (), on: 2013/8/15 12:00**

Yahoo has the same issue:

[http://news.cnet.com/8301-13578\\_3-57587463-38/the-yahoo-e-mail-privacy-flap-that-wasnt/](http://news.cnet.com/8301-13578_3-57587463-38/the-yahoo-e-mail-privacy-flap-that-wasnt/)

A friend of mine who works in high level programming let me know that absolutely nothing that is sent over the internet is private. It is my understanding that the same is true for voice, text and fax transmissions. None of it is actually private.

**Re: If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy' - posted by RobertW (), on: 2013/8/15 13:07**

Interesting and disturbing.

**Re: , on: 2013/8/15 13:20**

Are there any options for private emails?

Bear.

**Re: If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy' - posted by SHMILY, on: 2013/8/15 14:17**

When my children were younger I told them not to put anything in writing they wouldn't want their mother to read.

Now I am older. I don't want to put anything in writing (or say or think or do) I wouldn't want the Lord to read. Others don't matter. I only answer to Him.

REJOICE! =)

Mary

**Re: , on: 2013/8/15 14:21**

The most realistic option for achieving private e-mails is to have a set of private and public encryption keys. The private key is held by the sender and the public key is attached to every e-mail sent. The recipient also has to have a set of keys of their own as well. This then allows both sent and received e-mails to be encrypted which makes for privacy between the sender and the recipient. For this to meaningfully work believers have to take their security seriously and encourage one another to get a set of keys.

If any one wants to get a set then I can initiate a generation process on a key encryption certificate server and the process will be fully automatic from that point on as far as issuing the Security Encryption Keys.

There are a few configuration issues and most likely this will mean using an SMIME e-mail client rather than using the usual auto configuration service provided by Gmail and some other providers. This is however really very simple and again if I know the e-mail client of preference and the OS platform (Windows, Linux or Mac OS X) it will be very easy to accomplish.

Or go to GlobalSign and look into their Personal Sign 1 Service. If there is support I would be happy to setup a certificate issuing authority just for believers which could be completely free of charge. Otherwise the usual cost of purchasing a set of keys is around \$15.00 per annum.

**Re: , on: 2013/8/15 17:33**

Quote:

-----by SHMILY on 2013/8/15 11:17:40

When my children were younger I told them not to put anything in writing they wouldn't want their mother to read.

Now I am older. I don't want to put anything in writing (or say or think or do) I wouldn't want the Lord to read. Others don't matter. I only answer to Him. REJOICE! =)

Mary  
-----

There are many things that my mother can read that I don't want Google, NSA, IRS, FBI, HUD, Homeland Security or FEMA to read.

**Re: , on: 2013/8/15 18:04**

Lorddoitagain,

It is true that nothing is private, anymore.

**Re: If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy', on: 2013/8/15 18:12**

beloved brethren,

this is all to be expected, ALL tying into prophecy in the Word of God...covered in Detail, in the Revelations of John.

I don't want to waste bandwidth, or bore any of you, by a long turgid posting, simply put, all of this, the terrible signs we see today, in every facet of life...in this WORLD, all tie in to the dictates of the whore of Babylon. (I simply refuse to capitalize that name...its a fell title, full of venom and wickedness)

have you noticed, that even in the popular entertainment of the day, what a prominent role several areas of "thought" play in the public marketplace?.....one sees "zombie" or "vampire" movies expanding in many 'offerings' out there, including secular based "end of the world" films.

one sees many shows that worship money.....for the last two decades...the stock market has received undue attention...a drama unto its own, with its own channels....and for the less cunning, there's always "game shows".

back to films, have you noticed the films, that show EXPLICITLY ...the govt as an out of control entity, that is the BAD GUY, intent on killing the GOOD GUY?...and many point to this as an example of our "freedoms"....as shown in the news today, and the very title of this thread...the truth in these films is undisputed, but notice HOW the filmmakers construct

he film.....they portray the govt as being absolutely OMNIPOTENT...and wicked...and our "good guy" barely makes it through the story of the film ALIVE...to the point where WE, the audience, breath a sigh of relief and think, "whew! glad that's NOT ME!"....the underlying message being.....don't mess with THE MAN....a not so subliminal message masquerading as a free 'exchange of ideas', when all it really is, at the heart of it...an ANTI Christ message...

meaning do we worship the state and worship power/money?

OR do we worship The Christ of God, Jesus?

I am NOT speaking of "rebellion"...i'm speaking of SEPERATION.

Bless God, I've had the opportunity..Divine Opportunity to REALLY dig deep into the Psalter...and what I keep seeing God say, and Speak of is..."to take refuge IN HIM"...."to WAIT on the LORD"....and I am at a point in my walk with Jesus, where ALL I want to do, is to take refuge IN HIM.

that's what I mean by separation...I am His, and His alone...its the world, the flesh and devil that nailed Him to That Cross, that Cruel Tree...the world, the flesh and the devil....and they had NO POWER over the Resurrected Son of God, Our Savior, Jesus.....so, Jesus living in me, that Glorious Reality...means this wickedness has NO POWER over me.

they can read my emails, they can torture me, and yes, they can kill this body, this jar of clay, but my soul?

He keeps....my soul belongs to Jesus, to God the Father, and one Day, we shall all be in the Heavenly Jerusalem.

in one of the very few worship songs I like, my sister Misty Edwards, glorifies Jesus, and just blesses my heart with this beautiful song, "Only a Shadow", which I can say "Yes and amen" too. I love you all in Jesus' love, neil

<http://www.youtube.com/watch?v=RKOQSpfFASQ>

**Re: , on: 2013/8/15 18:36**

Amen, Neil.

The only true separation is being IN HIM.

**Re: - posted by TMK (), on: 2013/8/15 18:51**

I have never had any expectation of privacy in emails, texts etc. Are people still that naive? I continue to use email, text etc because i dont write anything that i would be horrified if someone other than the intended recipient read it. I dont think my emails are very exciting. Besides there are billions of other emailers who also have to be monitored. You have to ask yourself...is the convenience worth the risk?

And remember we never have any expectation of privacy...the Lord is always watching even when Big Brother is not.

**Re: - posted by Lordoitagain (), on: 2013/8/16 10:53**

Dan 2:28 But there is a God in heaven that revealeth secrets, and maketh known to the king Nebuchadnezzar what shall be in the latter days. Thy dream, and the visions of thy head upon thy bed, are these;

Dan 2:29 As for thee, O king, thy thoughts came into thy mind upon thy bed, what should come to pass hereafter: and he that revealeth secrets maketh known to thee what shall come to pass.

Dan 2:30 But as for me, this secret is not revealed to me for any wisdom that I have more than any living, but for their sakes that shall make known the interpretation to the king, and that thou mightest know the thoughts of thy heart.

\*\*\*\*\*

Dan 2:46 Then the king Nebuchadnezzar fell upon his face, and worshipped Daniel, and commanded that they should offer an oblation and sweet odours unto him.

Dan 2:47 The king answered unto Daniel, and said, Of a truth it is, that your God is a God of gods, and a Lord of kings, and a revealer of secrets, seeing thou couldest reveal this secret.

Mar 4:22 For there is nothing hid, which shall not be manifested; neither was any thing kept secret, but that it should come abroad.

Luc 8:17 For nothing is secret, that shall not be made manifest; neither any thing hid, that shall not be known and come abroad.

Mat 12:36 But I say unto you, That every idle word that men shall speak, they shall give account thereof in the day of judgment.

Mat 12:37 For by thy words thou shalt be justified, and by thy words thou shalt be condemned.

**Re: - posted by ginnyrose (), on: 2013/8/22 20:42**

Since this is true, is it possible for someone to listen in on my conversation if I have my cell phone nearby but turned off?

**Re: - posted by ginnyrose (), on: 2013/8/22 20:43**

Since this is true, is it possible for someone to listen in on my conversation if I have my cell phone nearby but turned off?

**Re: - posted by Sidewalk (), on: 2013/8/22 23:46**

They see you when you're sleeping,  
They know when you're awake,  
They know if you've been bad or good,  
So be good for goodness sake...

Little did we know that the kindly looking fat man in the red suit would turn on us and hand over everything to the NSA!

**Re: If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy' - posted by Lysa (), on: 2013/8/23 10:21**

There is no expectation of privacy anywhere, not even in our homes or vehicles! If we send snail mail, someone could tear it open and read it. Those little red or blue lights on our BlueRay players, laptops and xbox's, tv's ... can look directly into our homes and watching what we watch and do and say!!

This might be a challenge one day for people naming the name of Christ... if you were arrested for being a christian, would there be enough evidence to convict you?!! Or would they just move on to the next house looking and watching? So something to think about!

God bless,  
Lisa

**Re: - posted by ginnyrose (), on: 2013/8/23 14:54**

Maybe NSA should take lessons from Santa Claus? Wish they would: Santa does not exist so by extension NSA would not either. Too bad??

Back to my original question: can NSA listen in on our conversations with a cell phone nearby that is turned off? We have no TV for them to peek in. The closest thing we have to is a screen is the computer. We do not even have internet on our cell phones - think the cost does not justify it.

ANOTHER question: would a corded land-line phone be safer for the exchange of information? I know if some have a scanner they can pick up conversations spoken through a cordless phone. SO, what kind of phone is the safest from probing ears?

Hey, this issue is much worse then when we had party lines where you heard everybody's phone on your line ring and you could pick up the phone and eavesdrop.. Yup! remember it well! :-)

ginnyrose

EDIT: Is there any electronic device one can own that cannot be used to snoop by an outside party?

**Re: The listening - posted by Sidewalk (), on: 2013/8/24 0:32**

Shortly after the identities of the Boston pressure cooker bombers was known, the police set out to find out just how wide the conspiracy was.

It was reported that they would be retrieving the cell phone conversations of Tsarnaev's (sp?) wife to see if she had spoken anything that would indicate she was in on the plot.

Then there was this pregnant pause-- "Oops!" They didn't want the public to know they could do that! The issue dropped like a bad joke at a funeral.

It was right about then the news began to break that the NSA was gathering all the phone calls, first they said it was just records that calls were made, then a further leak revealed that they are gathering content as well. They have very sophisticated ways of spying on the public, while constantly reassuring us that is for our own good and public safety.

With fingers crossed, they are hoping we will buy it. And some are.

In reality, the political corruption in this and other countries runs so deep now, they can't afford to just be honorable public servants. There are so many hands in so many cookie jars- and it gets worse every day. Money is being borrowed, printed, stolen, and redistributed so fast no one can keep track. The crash is inevitable, and a Spiritual revival is the only alternative to wholesale devastation.

Probably just preaching to the choir here, but each of us needs to be aware of what is coming down the track at very high speed.

By the way, if you visit Washington DC and view the White House across from Lafayette Park, you will notice just a simple black iron fence separates you from the White House lawn. But if you stick your hand through the fence to snap a picture of the building with your cell phone, you will notice that it has shut down. Force field. And You have been both seen and photographed. They know who you are already.

My limited understanding, Sandra, is that if you are not actively speaking on your cell phone, the spy agency cannot hear you. If the phone is on however, they are probably able to determine your location by triangulating local cell towers in range of your phone.

Smart phones are another animal, and I think I read somewhere they can activate them remotely to be able to hear ambient conversations when you are not aware. I could be wrong on this, but you can bet they are working to make it a reality. This tiger is out of the cage, who knows how sophisticated it will get.

The NSA has no sense of humor.

**Re: - posted by ginnyrose (), on: 2013/8/24 9:42**

QUOTE:

---

Smart phones are another animal, and I think I read somewhere they can activate them remotely to be able to hear ambient conversations when you are not aware. I could be wrong on this, but you can bet they are working to make it a reality. This tiger is out of the cage, who knows how sophisticated it will get.

---

Ok, we do have a smart phone, a low end model. It can do marvelous things besides make phone calls - access the web, take pictures and who knows what else?? But all we do is talk, text and take a few pics - got another camera for that.

One thing I have been noticing in recent days is how the thing will turn on without me doing anything to it! I keep it turned off and if idle for any length of time will shut off by itself. An incoming call or text will turn it on and then it will either ring or beep.

The worse thing about it is that when we got it there was no user manual - one had to go online to access it. Oh, sure there was a small booklet that taught you how to turn it on, but that was about it. We were about to throw the thing because of frustration. But we learned - slowly.

So....what am I to think if the thing turns on by itself for no apparent reason?

**Re: If You Send To Gmail, You Have 'No Legitimate Expectation Of Privacy', on: 2013/9/12 1:44**

Having read your insistence that all internet data is vulnerable to US government snooping and that there is no communication which is safe I have read into this a little further.

What I have read tells me that whilst it has been reported in the press on the back of recent leaked NSA & GCHQ documents that there are three areas of application to the NSA & GCHQ undermining of the SSL protocol technology layer, as well as personal privacy and commercial privacy, the actual facts are sparse and ambiguous. On a closer reading of the claims I believe that the issues of privacy both commercially as well as individually is undoubtedly true. The claim regarding the SSL/TLS protocol is very unlikely to be true in my opinion. The claim amounts to saying that the efforts of the NSA primarily represent undermining the protocol itself by having code inserted into the protocol via development, in cooperation with developers as far as algorithmic paradigms are concerned as well as manipulating the NIST as far as standards are concerned.

The actual accessing of data appears to have been a mixture of court judgements as well as commercial cooperation with some of the main players in data storage. It would appear that there has been only a relatively small amount of effort implemented on SSL activities or "code breaking" in the form of super computers designed for that specific purpose. Even this is a "battering ram" approach and has nothing to do with mathematical developments giving rise to vulnerabilities in existing cryptographic paradigms.

I cannot find a single shred of evidence that any mathematical development exists which has overtaken the SSL algorithmic paradigm. What I have found is that SSL (TLS) and S/MIME appear to share the same vulnerability by reason of their common 256 SHA Key requirement. There is no evidence that anything other than meta-data has been read from e-mails however. The contents cannot be read where the e-mail is encrypted unless you have the "master" keys. Proof needed.

And this is the point really. Of all the claims being made about the NSA and GCHQ, the only one which should really concern anyone or surprise anyone is the claim that the NSA has "somehow" altered or restructured the SSL/TLS protocol in collusion with the public standards agency (NIST). See <http://blog.cryptographyengineering.com/2013/09/on-nsa.html> "Which Standards" Paragraph.

I am not convinced that the reporting of this NSA & GCHQ activity and ambition, along with its successes is sufficiently well understood, and so it gives rise to a claim that all cryptographic exchanges are flawed and therefore useless. I would simply encourage anyone who has an interest to read the articles available (mostly in the press) and recognise the language being used. See <http://www.nbcnews.com/technology/after-nsa-encryption-cracking-revelation-can-we-trust-internet-security-8C11092386> .....it is full of euphemisms and slights of hand as usual and in reality amounts to a few short claims which ought to surprise no one at all. What is more, no one in the computer security industry is surprised by the majority of it. The only real surprise is the claim that SSL/TLS is compromised internally. Even this has to be qualified as the NSA has shown its hand before. See <http://www.zdnet.com/has-the-nsa-broken-ssl-tls-aes-7000020312/> para 9. And whilst this "antecedence" is clear evidence of the NSA's methodologies this still does not amount to proving that the NIST has cooperated with the NSA in guaranteeing that private and commercial security is compromised by default.

The claim that the Secure Sockets Layer itself has been "managed" so as to have loopholes built into it, is unproven. Where data and e-mails have been harvested it has been done primarily via tapping into Tier 1 servers and VPN Tunnels with consent or else by reason of court orders.

<http://siliconangle.com/blog/2013/09/09/google-strengthens-its-encryption-methods-to-hinder-nsa-espionage/>

## Strong Cypher Encryption Works!

The first link below reports on an interview with Mr Snowden who provoked this present crisis, in which he confirms that despite everything “Encryption works. Properly implemented strong crypto systems are one of the few things that you can rely on. Unfortunately, endpoint security is so terrifically weak that NSA can frequently find ways around it.”

<http://www.theguardian.com/world/2013/jun/18/edward-snowden-live-q-and-a-eight-things>

In other words a competent use of security at the ISP (end point) would guarantee security because cryptographic key encryption works. “Properly implemented strong crypto systems are one of the few things that you can rely on” is a very telling phrase coming from a former contracted Administrator of the NSA. It is also very telling that the NSA has now released 900 other Administrators from their contracts, leaving them with just 100 such contracted personal. They are moving their system into a cloud based remote machine management system to remove the human risk of another Mr Snowden. If you or I were simply seeking to achieve a secure and private platform fire walled through to the internet bypassing the ARPA requirement for DNS resolution, it would be a simple matter to build such a communications network.

## US Reporting

[http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&\\_r=1&](http://www.nytimes.com/2013/09/06/us/nsa-foils-much-internet-encryption.html?hp&_r=1&)

I would still bet my last dollar that much of the claims being made have yet to be properly qualified and in the end we will find that its been a good story about privacy and not as some are claiming NSA genius in defeating internet security per se. It is ironic that the majority of “scary” reports are giving a heads up to the Guardian in the UK for the “leaks” concerning the NSA. However just read the UK press and then compare it with the USA press. The one is mildly indifferent and amused. The other is full of fear tactics. Too much Hollywood as usual?

I am not sharing this to be argumentative but the question has been raised about how secure e-mails are because of the stated position of g-mail in the OP (now removed) and not because of NSA activities. Although the relevance of the disclosures regarding the NSA is obvious, it would not matter one bit if g-mail were citing a legal precedent with the intention of handing the information over freely or else preparing us for the fact that they already have done. This is because if they are legally required to do so their commercial well being is entirely dependant on cooperating with the NSA.

Setting aside my joke about breeding pigeons earlier, I also think that it is missing the point a little to assume “Christians” need have no concerns. We have a command to be as cunning as serpents in our understanding of worldly realities, whilst being as innocent as doves in our conduct and intentions. The recent conference “Sleeping Virgins and the Soon Coming of Christ” brought out several interesting points in this area of reality with regard to North Korea and China. I have no doubt that when the time comes we will find that some brethren have already been preparing!

If you encrypt your e-mails they cannot be read by anyone else unless they steal the private keys. Keeping those keys secure will be the real security. What we need is a Certificate Issuing Authority that is trustworthy in the sense that its directors are willing to go underground rather than compromise others. Technical pastors as it were. Not one but a number of them. The internet is already beyond any one group of interested parties, nations and individuals, regardless of wealth and knowledge. No one is going to let it fail. So if it not allowed to fail commercially; and given that it is latency driven, it is likely to stand. That and a private mailing system or two should be helpful as well then we can be rid of the money men and our dependancy on them. Get rid of the power to control by money and you have done much to get rid of the bogey man!

The following URL’s link to an extended blog article written by John Couzins who is a British Security Expert and make a easy reading of the issues involved.

<http://johncouzins.wordpress.com/2011/06/27/the-history-of-sslts/>

<http://johncouzins.wordpress.com/2011/07/11/technical-implementation-attacks-on-sslts/>



<http://johncouzins.wordpress.com/2011/07/31/certificate-weaknesses-in-sslts/>

<http://johncouzins.wordpress.com/2011/08/11/human-weaknesses-in-sslts/>

<http://johncouzins.wordpress.com/2011/08/17/conclusion-on-sslts/>

If you managed to read all of these links you will realise that the Internet is a human device and the only rock solid stability is that of Math and its underlying certainty. The whole issue of the NSA is essentially not a technical issue per se, it is a human issue right down to the transport layers themselves and their original limitations. It is also possible to imagine that an Intelligence Agency with sufficient resources could exploit both the technical vulnerabilities of the original and developed transport and security layers of the OSI model building on the weaknesses of the TCP/IP stack.

[http://en.wikipedia.org/wiki/Internet\\_protocol\\_suite](http://en.wikipedia.org/wiki/Internet_protocol_suite)

As all intelligence gathering agencies have limitations as to what they can and cannot achieve in the real world so those who use these same resources can also understand the weaknesses as well. If the weaknesses can be exploited and understood it must also be possible to implement best practise and at the same time "fill out" that knowledge with human intelligence of the ordinary kind. That is to say "be ye as cunning as serpents".

When I spoke earlier of the recent SermonIndex Conference I was speaking about two things primarily. The first is the rather graphic description which Edgar gave of the 24 brethren who were rounded up because their names were written in the folds of a bible. The pastor and the elders lost their lives in a truly terrible way. Thank God all such sacrifices work for good with the Lord, but would we ourselves want to put other brethren at risk simply because we did not exercise wisdom. The other reference was with regard to China and the removal of the SIM card from the phone itself as a mechanism to deter tracking technologies in meetings. When I heard these two things I was reminded of Paul after his conversion on the Damascus road and his escape from Damascus with the help of trusted brethren through a gap in the city wall at night. On arrival in Jerusalem he was feared by the brethren and had to be taken to the apostles and formally tested by them in order to establish a basis for trusting him. After this it is said that Paul went about the city freely according to the measure of time given him, and then was moved on by other trusted brethren. The conclusion was that there was peace and fellowship in the city of Jerusalem in those days despite the efforts of the Pharisees to murder both Paul and the other apostles.

It is remarkable to me that the brethren in Jerusalem were not able to discern that Paul was a true believer and therefore to be trusted. How much more if these brethren in Jerusalem in the days of the apostles were not given to know that which would ordinarily be seen as essential for their welfare, must we be vulnerable to wolves and deceivers in our day? We can spiritualise these things if we desire, but to do so would be to deny a reality. If God is to be sovereign in our lives we must be real in our own lives as well. We are not puppets or play things. We are the children of God and have a true part to play in working out our own salvation and the salvation of others. It is God's will that we cannot know that which belongs to God. We have to trust and we have to distrust as well. It is only in being real with others and expressing that reality which makes for the sovereign work of God in our own experience.

Britain and the USA have been the harlots of the world since the 18th Century. Britain devised this harlot system and the USA has made a brothel of it. Lets get real. Our nations are dogs and whores and that's a fact. We love money and we love lots of it. It is for our own gratification. We are beasts with it and ravenous wolves without it. When we think we have not enough we go out and devour for it. We will sacrifice everything without exception to make money and we will kill anyone to keep it. I would like to think that Britain is somehow a lesser harlot than the USA but alas I think I am deluding myself.



**Re: - posted by dohzman (), on: 2013/9/12 15:38**

You are correct:) what many people do not understand is that way back when Ma Bell had her land lines going the software are to pick out key words and zero in on those conversations already existed. That has been in place way before the mid 70s. Much of what we are seeing now is just because information is so much more available and accessible to the average person. Something happens now days, it gets posted on YouTube and next thing you know it has 1 million hits. I work in networking and am presently working toward security certs in Cisco, so when you see many of these articles sometimes you just have to shake your head because at the end of the day no matter what internet/intranet.....someone somewhere can view what is being transmitted. The main thing to remember is that 99% of us will never be on a watch list and to fixate on things like this will only lead to insecurity and paranoia.