All.Net Analyst Report and Newsletter

Welcome to our Analyst Report and Newsletter

It's how you use it that counts – and GDPR

I recently reviewed the Google policies on information collection, sharing, and use. Here's the thing… you can control who get what (in some cases), but you cannot control the use. And to me, that's the key. I don't really care who gets information as long as the ways they use it are limited to acceptable uses.

They had no choice

The Internet service providers, in anticipation of the General Data Protection Regulations of the European Union (EU GDPR), are notifying their users of the (new) rules.

Here are some (*selected*) quotes (*comments in italics indented*):

> "As you use our services, we want you to be clear how we're using information and the ways in which you can protect your privacy.
>
> *They say this, but the reality is quite different*
>
> … We use the information we collect from all of our services to provide, maintain, protect and improve them, to develop new ones, and to protect Google and our users. We also use this information to offer you tailored content – like giving you more relevant search results and ads.
>
> *"…like…" i.e., including without limit, i.e., all sorts of other things not disclosed*
>
> … Our automated systems analyze your content (including emails) to provide you personally relevant product features, such as customized search results, tailored advertising, and spam and malware detection."
>
> *"…such as…" i.e., all sorts of other things not disclosed*
>
> … People have different privacy concerns. Our goal is to be clear about what information we collect, so that you can make meaningful choices about how it is used. For example, you can:
>
> *Not one of the items listed below indicate you can control **the use of** the information shared, including with third parties.*
>
> … Many of our services let you share information with others. Remember that when you share information publicly, it may be indexable by search engines, including Google. Our services provide you with different options on sharing and removing your content.
>
> *They don't mention what happens when they share it. How they or others may use it.*
>
> … after you delete information from our services, we may not immediately delete residual copies from our active servers and may not remove information from our backup systems.

> *In other words, even if you tell them to remove it they still have it, for example, in backups.*
>
> … We do not share personal information with companies, organizations and individuals outside of Google unless one of the following circumstances applies: … For external processing… We provide personal information to our affiliates or other trusted businesses or persons to process it for us, based on our instructions and in compliance with our Privacy Policy and any other appropriate confidentiality and security measures.
>
> *Note that they do not list who those partners are or what they share with those partners or how it is used.*

What is not transparent here?

Now to be clear, I think Google does a better job than most in this arena. However, here is what **they do not disclaim and might do** by, for example, using detailed content of emails, locations, voice recordings collected when you didn't even ask for it, and/or search results to:

- Analyze psychological properties, and use results to serve directed propaganda to affect elections.
- Determine when you are pregnant and use results to send anti- or pro- abortion information.
- Determine that you are unfaithful to your significant other and tell them such.
- Sell information on your business, like internal plans and negotiation details, to competitors.
- Provide the news media with your internal online discussions.
- Provide robbers with the list of folks who live in your house and their real-time locations, and details of what you have purchased.
- Tell your customers what you really think of them.
- Tell the folks you are on a call with the things you are saying when on mute

The list goes on and on…

Use control

In truth, I don't think (and hope not) that Google does these things. But based on history, others do. And to me, the issue here is not privacy or sharing, although they play into it. The real issue is controlling the use of information.

I think that any service that wants to be "transparent" should list every thing they actually do with every piece or type of information they have, and that the user (you and I) should be default opted out of all such uses. A simple checklist of what they want to do should be provided, and the "what" in simple terms such as those in my list above should be clearly stated. Then you can check off what you want to allow and they cannot use your information for anything else. The list should be complete, and not include terms such as "like" or "including" but rather list every actual use.

What's good for the goose is good for the gander...

My system policies

My online policies as stated on my Web sites:

> *"The user of this computer has no expectation of privacy. We regularly monitor all input, content, and output of this computer and reserve the right to do anything legal with any of the information we gather. "*

I think that's pretty clear and transparent. If you tell me, I will do whatever I want with it. That includes all of the (legal) things listed above and any- and every- thing else you or I or anyone else might imagine, as long as it is legal. If you don't want this, don't tell me anything!

> *I don't want to stop Google or anyone else from doing legal things.*
>
> *I just want them to be transparent in reality.*

Don't claim to be transparent – be transparent

This is the real problem I have with online services.

- I provide an opt-out. Don't use my services unless you want the "ANYTHING" result.
- Google doesn't provide an opt-out with transparency.

Like so many others, they give us innocuous examples. They act like they are doing things only for our benefit. But they don't mention the stuff we might not want them to do. And if you try to find these things out, they will not tell you. I tell you: if you can imagine it, I might do it.

And to reiterate, while I am using Google as an example, they are, as far as I am aware, less exploitive than many others – historically way better than Facebook (which sells the details to all sorts and has failed to control it) or Twitter (which has historically sold of all the tweets to anyone who is willing to pay for it) or … you get the idea.

What's the reality?

- Today, I don't do anything with any data you provide to my sites other than provide the services directly resulting from your input that you see the results from. I save the input but not the analysis or the output (except on some sites which have more detailed contracts for special purpose uses). And I don't intentionally share it with anyone. But you know, it's the Internet and I don't control what my ISPs might do.
- Tomorrow, I might do anything else, and I might not tell you about it. Or at least I won't intentionally be obligated to tell you. In reality, I probably will tell, but don't count on it.

Conclusion(s)

Trust me – I might do anything. **Don't trust them** – they tell you that they don't tell you and try to make it seem like they do tell you and that it's innocuous – history shows it often is not.

It's about how they use your data – and you. And likely, what you really care about is how they **USE** the information, not merely what they collect or share or with whom.

It's not free! You pay for it. The way you pay is that they exploit you and/or your data to make money, often from someone else who exploits you or your data to make money. It's exploitive!

What I think we mostly want and don't get is "**use control**" - control over how our information is used. Perhaps if we aim at the right target, we might start to hit it…

A follow-on

Here is an email I just sent in response to a company that notified me of the new GDPR changes they were making:

> I looked on your privacy page but it provides no method I could identify other than this to control my privacy settings.
>
> I wish to opt out of everything I am able to opt out of while still using your services.
>
> I also wish to have a complete record of all information you have on me and everyone you have shared it with.
>
> I wish to have specific clarity around all of the policy elements that provide examples rather than comprehensive lists of what you do, and all of the ones that were not definitively specified.
>
> I want to make certain that any time you propose to share anything else with anyone else, you by default do not share my information with them unless and until I have given explicit permission, including the details of the specific uses, and that before you share they agree to all the same terms and conditions herein.
>
> I wish to know all of the same information and have all of the same restrictions put on all information you have ever or ever in the future do share with anyone else and on all of the parties you have shared with, recursively through everyone they have shared with, and so forth.
>
> This applies to all accounts that I have with you.

I would urge you all to take similar action with respect to every account you have everywhere.

Our GDPR disclosure

I figure this is the right place to tell all of you about what we collect, do, and keep. So the first thing to know is that “we” includes Management Analytics, Fearless Security, Angel to Exit, The Cyberspace Research Institute, Monterey Incubator, Can Do Funds, Keiretsu Forum Pebble Beach, and all of the related companies and sites associated with all.net – which is to say this applies to all of the net things we do.

We use service providers: Currently Google, GoDaddy, Constant Contact, and providers you access to get in touch with us, ISPs (AT&T, Comcast, three cellular carriers, any WiFi access points we might access), phone companies, credit card companies, and others you use in dealing with us. Generally, we don’t send them information about you, you do.

What information we get and retain: We get what they and you send us and anything we find on the Internet. So if you go to a Web site or some such thing hosted by someone else, they may collect whatever you send to them, even if we don’t necessarily get most of it. When you fill out a form for one of these companies, we get the information they send us, and in some cases, we run the sites ourselves and we get all of the things you send us. So if you send it to us, we generally get it. Whatever we get, we retain, and by using those methods to deal with us, you can expect we might keep it forever and never get rid of it. Of course we don’t guarantee to keep it, and when we have no further business use for it, we may throw it out or not, depending on whether it’s easier to get rid of it or keep it. So as a rule, don’t send it to us if you don’t want us to get it, retain it forever, and selectively and at our sole discretion

or by accident, no longer have it. For basics, we should not that some of the information we get we might reasonably keep for 100 years or more, assuming we are still here to keep it. Some of it isn't retained for more than the few milliseconds it takes to process it through tie input device interfacing to the communications media it comes from. And we change our methods with time, so some things we used to keep we might not keep any more and other things we didn't keep might be kept now. You cannot count on what we might keep or not. We don't always know, so we cannot tell you.

What we do with it: We generally do whatever the information was provided to us for. This is normally dictated by contracts we have with our clients. For example:

- **We do forensics and litigation support work.** Whatever we end up getting, we use it to do that work. We may also use it for research, but if we do we won't release the data itself, only the conclusions, except of course that court orders or discovery requirements may require is to release it. We might search it, analyze it manually and/or automatically, examine it in different ways, reconstruct things, operate programs in reconstructed environments, copy it in different formats, mount and unmount it and sub-file systems, unzip zip files, look in empty file space or otherwise unused or hidden parts of disks, and on and on. Some part of it we may never get to or understand or characterize or be able to decode, decrypt, or understand. It might contain evidence or instrumentality of a crime or the basis for civil or administrative action. We may be required to retain or destroy the contents and to not reveal what we have or its nature by a court of competent jurisdiction, contract, law, or regulation.
- **We do business development work.** We have forms people fill out on their businesses. They send us spreadsheets, PDF files, recordings, videos, slide sets, executable programs, data sets, and documents of all sorts and in all formats. We record sessions with them in some cases. Some of these are made available to others for use in evaluating companies, for advisory board work, to support our business development efforts, and so forth. We tell our clients about this and contract with them in this regard. This information may include all sorts of things we are not even aware of. For example, a Word document might include deleted personal or confidential information that we are unaware of, and we don't seek to become aware of it. Spread sheets may contain lists of people, amounts of money, financial information, or whatever they choose to send us. Forms the fill out for tracking efforts may include similar information. We don't control what people send us, and we don't keep track of all of the referenced parties or other information in things we are sent. We use what we get to do our business development work, in any way we see fit to do that work. And our methods change over time, so we might use things we got before to do new things with it. Or we might never use it again.
- **We do pathfinders and security assessments, sometimes including protection testing.** We use forms that are filled out in live remote online sessions and subsequently augmented in our locations or by our people to provide a reasonable and prudent future state. We may get additional information in any form our clients choose to provide it. We may enter facilities and get physical access to media, some of which we may retain and never know the contents of. We might do remote activities that end up with us possessing anything the customer possesses. We only keep track of it to the extent required to do our job, and we don't always try to figure out what's in it.

- **We do research, development, and education.** This involves finding information from anywhere we can identify as a source, analyzing it with whatever methods are appropriate to the effort, and doing whatever is required with it for the purposes of the research, development, or educational use. We don't always know in advance what we will do with it, but if it is for scientific research, we follow appropriate protocols for notice and informed consent associated with the nature of the research and sponsor.
- **We do all sorts of other stuff.** Too many things to even try to list here. Just like above, we get all sorts of information in all different forms and formats, and use it for the purpose of the effort we are doing for clients or for the internal uses of the effort under way. We may use it for other things later, but normally we don't.

As an overarching notion, we keep what anyone sends us, including in some cases in systems of records that do not provide for deletion – because they are intended to keep an accurate record of what happened over time. We take and keep notes related to things we do with clients, in most cases made available to them, but internal notes, emails, and other discussions as well. We also keep discussions surrounding contracts including forming the contracts, negotiations, deal terms, and all manner of other things, including notes on conversations, emails, posting, and so forth. We use this so we can accurately understand and recall what took place and advise based on the information made available to us. It also helps us be efficient and systematic in our work and not have to depend on our memory. We also keep track of things like sales and marketing data, financial transactions, invoices and payments, historical documents, draft reports, final reports, slides and draft slides, ideas, planning documents, corporate minutes, and just about everything else we do. So as a rule, anything we do or say or send or or receive, either internally or with you or anyone else, we might have notes on, and anything you tell us, we might have a contemporaneous record of. We may use it to do all sorts of things, but generally, we don't provide the results of anything we do with it to anybody else. That's because we do almost everything in confidence with our clients. We don't control what they send us and don't necessarily know what all of it contains.

What we don't do with the data we have: Generally, we are not interested in exploiting data about individuals or businesses to take advantage of them. We know that we might be able to get a bit more money out of our clients by using something like the knowledge of their birthday to make it seem like we are thinking personally of them. Of course we do try to wish everyone a happy birthday, because it's nice to be nice to people. And we say hello to strangers on morning walks and try to meet people in the room we are in when we go to meetings and workshops. But this is not data exploitation. It's just being nice. We don't put all of your data into a system and seek to find things out about you using deep learning AI block chain cloud big data methods. Of course some day we might try it, but that's not really our thing. We keep track of things like when we will next get in touch with you, so we don't miss appointments or forget to get back to you. But we don't do any automated psychological profiling of you to determine that we should call you Thursday at 2:35 PM or remind you of how much you like Baseball or anything like that. We do have a great tool called Decider and another called Influence designed to help make better decisions and determine how to effectively communicate with people and entities so as to achieve objectives. But we don't use it based on any of the data you send us, at least not these days. We have an application that does psychological analysis of the author based on their writings, but we only use it to let you find out how these systems work. We don't use anything anyone enters into it. Get it?

Who else gets it: We generally only share information with people we use as subcontractors for the purposes of the specific task. For example, if we are working on a consulting gig, the folks working on the gig may get access to the information related to that gig. Similarly, if we are working on a legal matter, the people authorized by the court to have access will be given access according to the court requirements, and for non-court mandated matters, the people working on the matter will have access to the things they need to have access to for their work. Generally, wherever it comes from might have a copy, and however it gets from us to you, the transport providers may get copies. So if we FedEx it to you, they might be able to open the package and make copies, but it's out of our control. We send names and email addresses to email providers, and of course they get the content of the messages sent back and forth. We cannot do anything about it. Same with our ISPs. If someone breaks into our systems, they may get access as well, and while we try to make sure this doesn't happen, no security system is perfect. As far as we know this has not happened, but if that changes, we will make it known. We may also send anything we have to our lawyer(s) or accountant(s) to the extent it affects any of the things they do for us. We may momentarily show example content from internal systems to 3rd parties as examples of what we do and how we do it. This will always be momentary, and generally be from examples of test systems, but there are cases where we show live data in small snippets over short periods of time.

What we can find: We don't necessarily know what information we may have about you, and even if we did, in some cases, we could not find or do anything about it. You know what we have about you if you sent it to us because you provided it. If you provided it to us in 1973, we may still have it, but we are pretty sure we would not be able to find it. Old tapes may not be readable, it may somehow be backed up to a disk drive somewhere, or encoded in a file format that is no longer processable, and we simply cannot do anything about it. And frankly, asking us to find it will only expose it to more people and potential to be remembered. Let sleeping dogs lie.

You don't know, and neither do we, if there is some data about you provided by or collected from one of our clients. And we don't have a good way to search for it. As an example, when we get a collection of a few million emails from a legal action and have to analyze them, we don't generally try to read the contents (unless we are asked to by the client). We would not know if anything about you was in there unless we looked for it specifically as a part of our work for the client. And we don't reveal the names of our confidential clients, except under court orders, so you wouldn't even know if we had a potential of having your information. Sorry about that. It's the nature of confidential working relationships.

But at the same time, if it resides on some disk somewhere in a safe deposit box in a vault, we are unlikely to ever have to access it, and it is far safer there than if we tried to get it off the backup media, loaded into our online systems, process and search it, and expose it to potential threats like computer criminals and government agencies. It's probably safer to not ask us to find whether we have something about you and just ignore the possibility as we do.

Eventually (perhaps not in our lifetimes), these media will be destroyed and the content lost. And usually within 10 years of making these backups, we will digitally erase the media and/or have it destroyed by a certified destruction company of some sort. Eventually…

We don't encrypt it all: When data loss is worse for us than data theft, we don't encrypt.

How you get in touch with us: Email generally works, but our phone number is also posted.

