Geolocation and Online Gambling

Proponents of online commercial gambling make a lot of claims, many of which prove to be half-truths, exaggerations, wishful thinking, or flat-out falsehoods. One such recurring claim is that, if a state will authorize online commercial gambling, the operators of the commercial gambling websites will ensure that only

(1) appropriately-aged people

(2) inside that state's geographic boundaries

will be able to engage in the online gambling. According to the online gambling proponents, the commercial gambling operators will employ technology to screen out or block non-residents and minors from online gambling (and, thus, from being exploited in the same way the operators' online gambling business aims to exploit local adults).

Analysis of online gamblers' IP (Internet protocol) addresses , usually via a process called "geolocation," is the supposedly-protective technology touted by the gambling proponents. The proponents claim this IP address analysis will tell whether the online gambler is in, or out, of the state and will also , with other information, help identify the gambler as being of the state's required age to suffer the social harms and financial losses engendered by commercial gambling.

However, there are more clear-eyed views of these proposals.

Unblinded by the prospects of profits, objective observers outside the commercial gambling industry--unbiased persons, who better understand how devices using the Internet are identified--recognize that entrusting geolocation capabilities to IP address analysis

(1) builds undue risks of error and inaccuracy into the system[1];

(2) masks "gaming" or "spoofing" the system; and

---

[1]

ENDNOTES

Much of this paper's critique of IP-based geolocation systems (or other IP-based Internet-user location efforts) adopts or re-words the Electronic Freedom Foundation's helpful explanation of the unreliability of IP addresses, alone, when they are employed in law enforcement officers' important tasks of determining the physical locations and identities of users of devices connected to the Internet. See, Mackey, Schoen, and Cohn, *Unreliable Informants: IP Addresses, Digital Tips, and Police Raids* (Electronic Freedom Foundation Sept. 2016)(accessible at www.eff.org). To minimize the number of endnotes (in hopes of maximizing readability), this paper does not cite every such usage from the EFF's paper. Instead, the interested reader is invited to review that informative work, which deserves much credit and from which this paper has extensively drawn.

(3) lulls regulators into a false sense of security—wrongly believing the online commercial gambling operators can screen out minors and out-of-state gamblers.

Testimony before Congressional committees has warned federal legislators of the limitations inherent in reliance upon IP address-based geolocation systems and how easily they can be spoofed,[2] but evidently some state legislators and regulators have either ignored or not heard such testimony. Some, too, may have been buffaloed or bought by lobbyists for online commercial gambling operators, as well as by the operators themselves and the geolocation firms who, seeing money to be made, brazenly oversell their capabilities.

Proponents of online commercial gambling legalization overstate the reliability of IP addresses as "identifiers." IP addresses have a limited technical purpose. These strings of numbers exist to identify a device (i.e., they provide an impermanent "address" for that device) on the Internet and to route traffic to that address. The use of IP addresses provides a simple, machine-readable system for rapid routing of international Internet traffic. Using this technology beyond the context for which it was designed, however, promises varying degrees of failure, since IP addresses identify only an Internet-based electronic destination. The physical location of that electronic destination is something that can be readily changed, spoofed, or misrepresented; furthermore, even absent such tampering, the electronic destination itself may be in motion or may be an IP address assigned to a device using a cellular tower that is inside one state while the device and its user are inside an entirely different state (a common occurrence near state borders).

IP addresses, never designed to uniquely identify a physical location, do not inherently "belong to" a particular country, state, or locality. While blocks of IP addresses are assigned to world regions by a coordinating body (the Internet Assigned Numbers Authority, or "IANA"), network operators known as Internet Service Providers ("ISPs") are usually in charge of further assigning IP addresses. No single standard exists among ISPs by which they assign IP addresses. Thus, an IP address need not be used in or from a particular physical location or area, nor by a particular ISP's end user.

While it is true that geography may factor into an ISP's decision on assigning local IP addresses, this factor (geography) typically only has importance to the ISP when geographic considerations prevail in network efficiency considerations. Since, invariably, the ISP's chief consideration will be creation and maintenance of the most efficient network process to deliver Internet traffic, whether locations near each other have like IP addresses

[2] https://judiciary.house.gov/wp-content/uploads/2016/02/Fagan-Testimony.pdf, pp. 3 & 12; http://docs.house.gov/meetings/JU/JU08/20150325/103090/HHRG-114-JU08-20150325-SD005.pdf, p. 3.

seldom turns on physical geography alone. Rather, where the ISP has its' physical links and routers usually plays a key role in determining IP address allocation.

It is also true, of course, that IP address allocations are recorded in searchable databases—yet it is just as true that these databases widely vary in content and comprehensiveness; moreover, as explained above, the significance of any IP address allocation can vary markedly. This is especially frustrating to efforts to reliably and consistently affix a geographic location to a device using a particular IP address. The frustration becomes even greater upon recognition that, *these days, devices often share a single IP address.* Neither is the situation helped by the fact that no central listing, map, directory, or cross-reference resource exists that pairs IP addresses and particular locations. Even if such a central resource did exist, *as time passes, IP addresses are frequently reassigned to different Internet users.* Neither is there any uniform method based on IP addresses of systematically mapping associated physical locations. While maps using such data can be created and, for some addresses, may prove accurate, necessarily the maps cannot be entirely comprehensive or correct, given the inherently inconsistent linkage between a physical site and IP address information.

Another flaw in use of the geolocation technique as a protective device for online gambling compliance is that users at both ends of the transaction have little motivation to consistently adhere to legal requirements. Each is willing to accept use of a technique that merely looks effective, since even a modest error rate inures to the financial advantage of the participants in online commercial gambling. The online commercial gambling operator wants as many gamblers as possible, to wager as much money as possible, as frequently as possible, and for as long as possible. Simply stated, that is the business model at the foundation of all commercial gambling ventures. At the other end of the online transactions, the gamblers gain the value they ascribe to the use of the online service, whether they win or lose their wagers.

Thus, if out-of-state gamblers or underage gamblers do use the operator's service, in the vast majority of instances the operator financially benefits (since, if playing against the house, it is the nature of the game that the gambler loses far more often than wins; and, if playing against other online gamblers, the operator collects a "rake" or fee from all participants in the wager). Hence, the operator of the online gambling entity is motivated to seek only that compliance technology that allows him to say "I tried," not "I succeeded," when it is later discovered that out-of-state or underage gamblers used the operator's online gambling site.

Likewise, the out-of-state or underage gamblers obviously lack motivation to insist on accurate compliance. They are likely satisfied, for example, that geolocation can be

spoofed or when it only works part-time to screen them out. After all, both occasional and addicted gamblers often feel they only need that one successful opportunity to bet what they feel is a sure thing, while sophisticated professional gambling conmen, point-shavers, match-fixers, syndicates, and their "beards" can be satisfied with strategically placing the occasional online bet from outside a jurisdiction, knowing that out-of-state investigations to locate and extradite them are costly and rare to the point of being effectively non-existent. Some legislators, too, hoping to maximize the revenue a state may make from taxing the online commercial gambling operators (whether the tax is based on the gross revenue , or "handle," the number of patrons, or both), figure that some form of modestly-successful compliance technology is "good enough," especially when the failure rate tends to fatten the state's bank account. Of course, this collection of persons willing to "look the other way" regarding commercial gambling law violations does little to promote respect for law, generally, and much to encourage its violation.

As for use of IP addresses in attempting to identify specific individuals (such as, for example, underage gamblers; persons who are on self-exclusion lists due to gambling addictions; persons suffering from mental illnesses or mental handicaps; persons banned from gambling due to criminal convictions and their associated pre-trial release, probation, or parole conditions; and persons using online gambling to launder money or finance terrorism or other criminal activity), *there is nothing about the IP addresses themselves that identifies anyone.* Again, IP addresses identify only devices or groups of devices on the Internet. With enough additional information beyond a known IP address, one can posit that a single identifiable person can be associated with a particular device connected to the Internet, but real-world contexts often defeat such conclusions.

One of the modern circumstances defeating such conclusions is that in most advanced and Internet-using nations, such as the United States, the most widely-used version of the Internet Protocol, IPv4, lacks sufficient available addresses to assign a unique IP address to each device connected to the Internet—there are simply more devices than there are available unique numeric IP addresses. This means that when an ISP's customers first access the Internet, they often will connect through an IP address that was previously used by someone else—or even through an IP address that is simultaneously being used by someone else! Technologies—particularly those used by mobile carriers providing ISP service and in household routers—now allow multiple devices and users to share a single IP address (e.g., Network Address Translation, or NAT, creates a private network wherein a single public IP address is shared by all the network-using devices).

To these problems, online commercial gambling operators may offer that technology changes, and these future developments may catch up and resolve these problems. Maybe, but maybe not. After all, already there is a new version of Internet

Protocol, IPv6. Yet, even with the much greater pool of IP addresses available via IP6, in the United States only thirty percent of Internet users have adopted IPv6 addresses (per measurement available at www.WorldIPv6Launch.org). Given the efficiencies of sharing IP addresses, neither IPv6's technological change nor reasonably-predictable others provide confidence that IP addresses will, in the foreseeable future, no longer be shared by multiple users and devices.[3] IP addresses simply are not static, do not identify a particular location on a map, and do not identify a particular person using a device.

Of course, with properly-corroborating information considered in conjunction with an IP address, it is *sometimes* possible to reasonably-reliably identify a particular location or individual. Using billing records obtained from an ISP and/or other location data (such as trace routing analysis, GPS report analysis from mobile devices, and real-world physical investigation to precisely match an IP address with a physical location), close, and sometimes precise, matching of an IP address and a physical location can occur. But online commercial gambling operators lack subpoena power to gain the billing records from ISPs (and citizens presumably would not want to give such powers to private entities), so this kind of data available to law enforcement is unavailable to commercial gambling operators.

ISPs can be expected to balk at bearing the added financial expense (i) of conducting labor-intensive physical investigations; (ii) of verifying, storing, and securing customer-supplied or investigator-discovered identifying information; and (iii) of risking costly privacy intrusions and thefts of these kinds of acquired personally-identifying information, or even that such as would be revealed by GPS and trace routing analyses. In any event, location information acquired from an ISP provider may merely reliably indicate the location of an ISP subscriber but not the specific user (who is gambling via that subscriber's broadband service). Likewise, even when the more complicated technical means of approximating an IP address and a physical location result in a "match," the result may not be an actual street address, and almost certainly would not reliably identify a particular person, his age, or other relevant circumstances.

Complicating the task of matching an IP address to an identifiable person is the widely-available existence of anonymizing services. Perhaps the best-known such service is "The Onion Router," more often referred to by its initials, Tor. As explained at torproject.org, Tor both masks the IP addresses of its users and routes the device's traffic

[3] Indeed, ongoing research suggests that technical revamping of the overloaded Internet, through development of entirely new, modified, or different addressing or operating systems or designs, such as Named Data Networking (NDN), could undercut or diminish even the limited utility IP addresses presently have in the effort to physically locate or identify users of the Internet. See, https://engineering.wustl.edu/news/Pages/Building-a-better-internet.aspx. Weight assigned to protecting internet users' privacy interests, as new technical changes are invented and refined, certainly will impact future identification and compliance tasks.

through exit relays that volunteers operate. These volunteers neither control nor have knowledge of the content, senders, or recipients of the Internet communications flowing through their relays. Online commercial gamblers using Tor provide revenue to online commercial gambling operators and minimize to the vanishing point their risk of being identified via IP address.

Further complications in identifying users stem from the now-common employment of open wireless networks operated by countless individuals, companies, and libraries, among others. These services typically have little or no control or knowledge of how the Internet connections they provide are being used, nor do they know the identities of the users. Even-more-complicating the challenge of using an IP address as a proxy for someone's identity is the existence of widely-available services such as proxy servers and Virtual Private Networks (VPNs). In short, multiple easily-accessed, often-used services exist to make IP addresses highly unreliable indicators of any particular person's identity and/or location.

Legislators and regulators also need to realize that when a device connected to the Internet is used on a different Internet connection, the public IP address associated with that device most often will change. Thus, as a general rule, one must consider that the IP address assigned to a particular subscriber's device may be temporary or dynamic, may include many other people's traffic, and some of these other people may be hundreds or thousands of miles from the subscriber's physical location. Hence, as a federal judge observed, "[I]t is no more likely that the subscriber to an IP address carried out a particular computer function…than to say an individual who pays the telephone bill made a specific telephone call."[4]

Responsible law enforcement agencies investigating cybercrime or seeking to locate suspects, victims, or witnesses know that an IP address provides merely the starting point of an investigation aimed at determining the person's physical location; typically, this initial clue must be supplemented with numerous pieces of additional information that the agency can acquire with subpoenae, interviews, surveillance, and other investigative techniques. *Responsible* law enforcement agencies do these things because they want to do things right, to ascertain the truth of an event, and to catch or locate the correct person. Mistakes waste their limited resources and can subject them to financial liability and public reproach. Often, their second step in such information-gathering will be to use a reverse Domain Name System (DNS) "lookup" of the IP address they have at hand. By checking this massive DNS database of the Internet's IP addresses and associated website domain names, investigators sometimes can find the name and contact information of the person or entity that registered the domain. This information, with additional investigative effort, may (or

[4] BitTorrent Adult Film Copyright Infringement Cases, 296 F.R.D. 80, 84 (E.D.N.Y. 2012).

may not) provide additional information about a physical address and, if so, still additional investigation may help determine if the address so located is, in fact, relevant to the goal of the agency's investigation.

In contrast, operators of online commercial gambling enterprises have motivations significantly differing from law enforcement agencies. Maximizing revenue and minimizing expenses, while adhering to the above-noted commercial gambling standard business model (to get "as many gamblers as possible, to wager as much money as possible, as frequently as possible, and for as long as possible."), is the overriding goal. Commercial gambling proponents frequently argue that framing the goal as just stated overlooks that protecting any existing legal authorization (license, permit, statutory authority, etc.) to operate their business is as, or more, important than the standard business model (since, if the authorization is lost through misconduct or malfeasance, the profit-making opportunity is entirely lost). Theoretically, that argument might seem valid, but real-world facts (e.g., commercial gambling's history of corruption; its' proven inability to adequately police itself; its' seemingly-magnetic attraction to society's grifters and criminals--both as employees and as patrons; and the actual experience of law enforcement and regulators with the commercial gambling industry's repeated defalcations and organized crime involvement), overwhelmingly establish that, when legal obligations exist that cut into profitability, this industry cuts corners whenever it can.

As observed in uncontradicted Congressional testimony (by a career federal prosecutor with extensive experience in investigating and prosecution online commercial gambling cases),

> At least responsible bricks-and-mortar casino operators can look a gambler in the eye and make the human assessment of whether he's too drunk, mentally unhinged, despondent and desperate, developmentally disabled, or otherwise at a point at which it's simply unfair to take advantage of him any longer. Internet gambling operators not only cannot assess these characteristics among their clientele, in my experience they don't care to, preferring to prey on the weak and the strong equally.[5]

No reasonable observer familiar with the facts expects that online commercial gambling operators will, can, or want to regularly conduct the kind of additional investigation that a responsible law enforcement agency conducts to reliably identify an Internet-user's address or identity and age. Some merely-cosmetic effort at going beyond the IP addres--at acquiring and verifying needed informati--is all that can be expected on a long-term basis. Indeed, that is all that the effort that presently is being expended in those

[5] http://financialservices.house.gov/media/file/hearings/111/fagan%2007-21-10.pdf

jurisdictions where some form of online commercial gambling *has* been authorized by incautious governments. And, knowing that states always lack the resources to investigate and compel compliance, *it is the nature of the commercial gambling industry to risk non-compliance, to avoid the expenses of self-conducted investigation, and to maximize revenue.* Industry protests and promises to the contrary are gossamer and short-lived.

There is no way that the federal government, or any individual or combination of state governments, can expand to the degree necessary to effectively police and regulate the likely scale of legalized Internet casino, poker, and/or sportsbook gambling (i.e., there will be millions of data transactions , informational and financial--involving billions of lines of code in malleable, disguisable formats with anonymizing and proxy tools readily available, use of manipulative techniques and subliminal messages, as well as easily-disguised traditional and electronic collusive and corrupting behaviors). Realistically: No police force/regulatory body will be big enough/skilled enough/funded enough [to effectively police and regulate the users and operators of online commercial gambling enterprises].[6]

Given that reality, and given the equally-certain disinterest of the online commercial gambling industry in conducting costly, comprehensive, and accurate IP address investigation, and given the frequently-misunderstood and limited purpose of IP addresses, no longer can one responsibly believe the online commercial gambling industry's "half-truths, exaggerations, wishful thinking, or flat-out falsehoods" regarding IP addresses.

(And this, of course, is entirely different than the industry's wholesale failure to explain how expanded Internet gambling would, somehow, make the world a better place for anyone--other than the already-wealthy operators of Internet gambling enterprises. That, however, is a topic for another paper.)

--The Predatory Gambling Liability Project, an effort of Stop Predatory Gambling, a 501(c)(3) organization;
October 6, 2016

[6] https://judiciary.house.gov/wp-content/uploads/2016/02/Fagan-Testimony.pdf, p. 3.